IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation, Plaintiff, v. SECURE COMPUTING CORPORATION, a Delaware corporation, CYBERGUARD, CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100, Defendants.	)	Civil Action No. 06-369 GMS

DECLARATION OF MEGHAN WHARTON IN SUPPORT OF FINJAN SOFTWARE LTD.'S REPLY IN SUPPORT OF MOTION FOR ENTRY OF PERMENANT INJUNCTION PURSUANT TO 35 U.S.C. § 283

OF COUNSEL:

Paul J. Andre
Lisa Kobialka
KING & SPALDING LLP
1000 Bridge Parkway
Suite 100
Redwood Shores, CA 94065
(650) 590-0700

Philip A. Rovner (#3215)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

Dated: May 16, 2008

I, MEGHAN WHARTON, declare:

1. I am an attorney with the law firm King & Spalding LLP, counsel of record for Plaintiff Finjan Software, Ltd. ("Finjan"). I have personal knowledge of the facts set forth in this declaration and can testify competently to those facts.

2. Attached hereto as Exhibit 1 is a true and correct copy of Trial Exhibit PTX-37, Secure Computing Corporation Product Meeting Minutes dated June 24, 2004.

3. Attached hereto as Exhibit 2 is a true and correct copy of a Microsoft Corporation press release entitled "Microsoft Advances Commitment to Secure and Seamless Networks at Interop" dated May 21, 2007, *available* at http://www.microsoft.com/presspass/features/2007/may07/05-21sandersqa.mspx.

4. Attached hereto as Exhibit 3 is a true and correct copy of Trial Exhibit DTX-1305, a letter from Paul Andre, counsel for Finjan, to Peter Watkins at Webroot Software, Inc., dated March 5, 2007.

5. Attached hereto as Exhibit 4 is a true and correct copy of Trial Exhibit DTX-1306, a letter from Wayne O. Stacy of Cooley Godward Kronish LLP to Paul Andre, dated March 26, 2007.

6. Attached hereto as Exhibit 5 is a true and correct copy of a conference call transcript of the SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call on May 1, 2008.

7. Attached hereto as Exhibit 6 is a true and correct copy of a document I created entitled "Finjan's Corrected Explanation of IDC Report Calculations." The information contained in this document accurately reflects the information contained in the source documents referenced therein.

8. Attached hereto as Exhibit 7 is a true and correct copy of a Finjan web page entitled "Technical Support Offerings," *available* at http://www.finjan.com/content.aspx?id=251.

I declare under penalty of perjury under the laws of the State of California and the United States of America that each of the above statements is true and correct.

Executed in Redwood City, California on May 16, 2008.

By: ______________________
Meghan Wharton

Exhibit 1

From:
To:
CC:
BCC:
Sent Date: 0001-01-01 00:00:00:000
Received Date: 0001-01-01 00:00:00:000
Subject:
Attachments:

FYI

-------- Original Message --------
Subject: Product Meeting minutes June 29, 2004
Date: Thu, 1 Jul 2004 17:30:00 +0200
From: Frank Berzau <frank@WEBWASHER.com>
To: Thomas Friedrich <thomas.friedrich@WEBWASHER.com>, Heiko Giesselmann <heiko.giesselmann@WEBWASHER.com>, Peter Borgolte <peter.borgolte@WEBWASHER.com>, Benita Sieben-Ostmann <benita.sieben@WEBWASHER.com>, Martin Stecher <martin.stecher@WEBWASHER.com>, Bart-Jan Schuman <bart-jan.schuman@WEBWASHER.com>, Tom Bryant <tom.bryant@WEBWASHER.com>, Horst Joepen <horst.joepen@WEBWASHER.com>, Christian Matzen <christian.matzen@WEBWASHER.com>, Jobst Heinemann <jobst.heinemann@WEBWASHER.com>, Gary Taggart <gary.taggart@WEBWASHER.com>

Participants: Peter, Roland, Benita, Heiko, Tom

1. State of Kentucky issues
2. CR status
3. WW status
4. Akonix

1) state of kentucky, Tom reports an issue with a lib with av, Tom to forward to Benita while Marek is on vacation

2) Maxdb integration making progress, db space mgtm missing
Feature discussion last week, no hot customer issues
4.3 targeted end of quarter, but will be later (maybe 10 days from today)

3) This week bugfix release with special feature for unicode handling
5.1 planning: Christoph and Jan started research proactive security features, also Roland doing research on proact. sec patents from finjan and trend
Urgent need for someone who does documentation. Cognitas (outsourcing docs) we will get a very good resource for three months, potential to extend.
Appliance: Frank will take CD to the sales meeting so we can demo

EXHIBIT
PENGAD 800-631-6989
37
GERMANY

Plaintiff's Trial Exhibit
PTX-37
Case No. 06-369 GMS

Spyware paper from Roland will be published on website today or tomorrow

4) Tom reports protocol updates with akonix failing

Exhibit 2

Click Here to Install Silverlight

United States Change | All Microsoft Sites

Search Microsoft.com for: Go

Microsoft

PressPass - Information for Journalists

PressPass Home | PR Contacts | Fast Facts About Microsoft | Site Map | Advanced Search | RSS Feeds

Microsoft News

- Product News ▸
- Consumer News
- International Contacts
- Legal News
- Security & Privacy News
- Events
- News Archive

Corporate Information

- Microsoft Executives ▸
- Fast Facts About Microsoft
- Image Gallery ▸
- Broadcast Room ▸

Related Sites

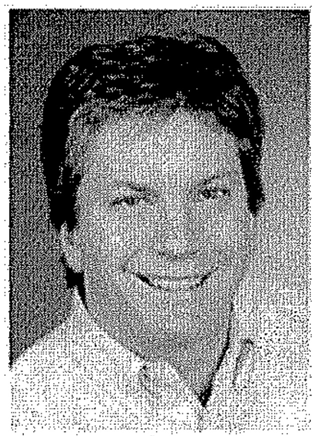
- Analyst Relations
- Community Affairs
- Essays on Technology
- Executive E-Mail
- Global Citizenship
- Investor Relations
- Microsoft Research

The PressPass Broadcast Room
Broadcast-standard media for download

Microsoft Advances Commitment to Secure and Seamless Networks at Interop

The company is working with the IT industry to provide network operators with greater access, security and interoperability.

LAS VEGAS, Nev., May 21, 2007 – This week at the Interop 2007 trade show, Microsoft announced that the company's Network Access Protection (NAP) technology will be interoperable with the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Network Access Control standard, which includes the NAC standards for Juniper Networks. This announcement represents a significant breakthrough for companies with diverse infrastructures and user needs. With this level of interoperability, companies can deliver access to users at anytime from anywhere, save money and simplify and improve network security management. Microsoft also announced the upcoming public beta of Intelligent Application Gateway (IAG) 2007 SP1, which contains some key enhancements to Microsoft's SSL VPN solution.



Henry Sanders, General Manager, Core Networking and Collaboration Group,

For some perspective, we turned to a longtime networking expert at Microsoft, **Henry Sanders**, a Microsoft Distinguished Engineer and the general manager of the Core Networking and Collaboration group in Windows Networking.

PressPass: What do customers want in regards to network security?

Henry Sanders: IT departments have users who seek a consistent connected experience, regardless of their location, the device they use, or the networks they traverse. At the same time, IT organizations need to deliver this seamless-access experience without compromising security or increasing complexity. In simple terms: it just works, works securely, and at a lower cost. Microsoft, driven both by these customer requirements as well as the needs of its own IT organization, is investing in solutions to deliver upon this vision of secure and seamless networking. One of the key components of that vision is NAP. Another is our SSL VPN product, the Intelligent Application Gateway (IAG)

Related Links

Press Releases:

- Microsoft and Trusted Computing Group Announce Interoperability – May 21, 2007
- Juniper Networks and Microsoft Announce Unified Access Control and Network Access Protection Interoperability – May 21, 2007

Virtual Newsrooms:

- Microsoft at Interop 2007 Virtual Presskit

Biography:

- Henry Sanders Biography

Microsoft Resources:

- Intelligent Application Gateway Web site

Windows Networking. Click image for high res version

2007.

PressPass: What is "NAP" and "NAC," what do these terms mean, and why are they important to IT?

Sanders: "Network Access Control" is a generic term that refers to a client/server method of ensuring proper health "posture" or "state" of endpoints before they can connect to a computer network. NAC systems usually include a policy server that checks the health state of a client attempting to connect to a network for things like up-to-date antivirus signatures or operating system patches. The NAC system can then limit access and/or remediate a device that does not meet minimum health requirements. .

Microsoft understands the importance of protecting networks from computers that do not meet corporate security policy, regardless whether the devices connect via a remote access gateway or locally via a wired or wireless LAN. This level of infrastructure protection will become a fundamental requirement for all IT organizations, and, in order to help our customers, Microsoft has developed an NAC solution called Network Access Protection (NAP).

Microsoft's NAP is a policy-enforcement platform built into Microsoft Windows Vista, Windows Server 2008 and Windows XP (update now in beta testing). NAP enables customers to better protect network assets by enforcing compliance with system health requirements. With NAP, customers can create customized health policies to validate computer health before allowing access or communication, automatically update clients to ensure ongoing compliance, and, optionally, confine noncompliant computers to a restricted network until they become compliant.

PressPass: Tell us more about this announcement, and what it means for network administrators?

Sanders: To put this into perspective, there are three primary NAC architectures. Microsoft's NAP, the Trusted Computing Group's Trusted Network Connect (TNC), and Cisco's Network Admission Control, or C-NAC. In September, Microsoft announced an interoperability agreement with Cisco's NAC solution. This week at the Interop trade show, Microsoft announced that NAP would now be interoperable with the Trusted Computing Group's TNC. The TNC agreement makes NAP's Statement of Health (SoH) protocol, included in Windows Vista, the standard client-server communication protocol within TNC. We are very excited because, with this announcement, Microsoft's NAP is now interoperable with the two other primary NAC architecture solutions, TNC and Cisco's NAC.

The SoH protocol now allows "client standardization," as organizations can now standardize on the (SoH) client protocol, regardless of their NAC infrastructure. The SoH client is available in Windows Vista, will be available in the next service pack of Windows XP, and through NAP partners for non-Microsoft operating systems. One of our NAP partners, Avenda Systems, is releasing a NAP client for the Linux operating system at

Enhancements for Intelligent Application Gateway 2007
May 21, 2007 – Microsoft today announced the technical beta of Server Pack 1 for Intelligent Application Gateway (IAG) 2007. The IAG 2007 SP1 contains a number of enhancements designed to help businesses deploy more secure and stable solutions for remote access to applications and data, including support for the Windows Vista operating system, support for Exchange Server push e-mail to Windows Mobile 5.0 devices, enhanced integration with Active Directory Federation Services (ADFS), and significant performance enhancements. IAG 2007 with SP1 will also fully

support Microsoft Forefront Client Security on both Windows XP and Windows Vista clients.

Along with the new integrated solution, Microsoft also announced five new original equipment manufacturing (OEM) partnerships with appliance manufacturing and distribution companies – Pyramid Computer Gmbh, nAppliance Networks, SurfControl, Mendax Microsystems and Baosight – joining existing partnerships with Celestix and Network Engines.

Interop. The broad level of interoperability removes a major adoption barrier by providing investment protection, because organizations can deploy NAP into their existing infrastructure without having to rip and replace their existing investments. The two key components of NAP, Windows Vista and Beta 3 of Windows Server 2008 are available now for companies to deploy and test.

PressPass: How does NAP fit into Microsoft's networking vision?

Sanders: NAP's integration as an industry standard is also an important milestone in advancing the vision of secure and easy "anywhere access" announced by Bill Gates at the RSA trade show in February 2007, as well as Microsoft's ongoing "Interoperability by Design" initiative.

"Anywhere Access" is Microsoft's call to action to design systems and processes that give people and organizations a high degree of confidence that the technology they use will protect their identity, their privacy, and their information. People increasingly want anywhere access that is easy to use and manage, with seamless, connected experiences that extend across networks and devices, so they can access, share, and use corporate and personal information without fear that it will be compromised, stolen, or exploited. NAP helps advance this vision by helping keep malware off networks, helping keep computers connecting to networks more healthy, and facilitating connections between networks.

"Interoperability by Design" is Microsoft's approach to interoperability, where Microsoft strives to bring technologies to market in a way that balances competitive innovation with an ability to connect unique systems and applications. As a result, technologies such as XML and web services, among many others, have evolved as industry standards, and the NAP SoH is now emerging as Microsoft's latest contribution to industry standards.

PressPass: Can you tell us about the Intelligent Application Gateway product?

Sanders: The Intelligent Application Gateway (IAG) 2007 features Application Optimizers, SSL VPN, a Web application firewall, and endpoint security management that enables access control, authorization and content inspection for a wide variety of line-of-business applications. Together, these technologies provide mobile and remote workers with easy and flexible security-enhanced access from a broad range of devices and locations including kiosks, PCs and mobile devices. IAG also enables IT administrators to enforce compliance with application and information usage guidelines through a customized remote access policy based on device, user, application or other business criteria.

PressPass: What's new in this release of IAG?

Sanders: The SP1 of IAG 2007 offers support for Windows Vista, which will extend to Windows Vista clients the IAG 2007's superb endpoint compliance tools, including, Download Manager, which helps enforce document and browser download policies based on user identity, location and end-point profile to avoid misuse of corporate data, and Attachment Wiper, the IAG 2007 cache cleaner which helps ensure that sensitive data is wiped from mobile clients when users close their sessions.

IAG 2007 improvements to enterprise integration include remote access support for Active Directory Federation Services (ADFS), which enables organizations to securely share a user's identity information across organizational boundaries. Other improvements include performance increases of up to 100% in certain HTTP deployment scenarios, and support for Kerberos Constrained Delegation (KCD), which simplifies authentication based on a broader set of client credentials.

↑ Top of page

Printer-Friendly Version Send This Page Add to Favorites

Manage Your Profile | Contact Us | Newsletter

Exhibit 3

Perkins Coie

101 Jefferson Drive
Menlo Park, CA 94025-1114
PHONE: 650.838.4300
FAX: 650.838.4350
www.perkinscoie.com

EXHIBIT
PENGAD 800-631-6989
PARR - 3
12-17-07

Paul J. Andre
PHONE: 650.838.4300
FAX: 650.838.4350
EMAIL: PANDRE@perkinscoie.com

March 5, 2007

Via Federal Express

Peter Watkins, Chief Executive Officer
Patrick Summers, General Counsel
Webroot Software, Inc.
2560 55th Street
Boulder, CO 80301

Re: Offer to License – U.S. Patent Nos. 6,167,520 and 6,480,962

Gentlemen:

We represent Finjan Software, Ltd. ("Finjan") in connection with corporate and intellectual property matters. Finjan is the assignee and owner of U.S. Patent Nos. 6,167,520 ("'520 Patent") and 6,480,962 ("'962 Patent), both entitled "System and Method for protecting a client during runtime from hostile downloadables." These patents may be relevant to Webroot Software, Inc.'s ("Webroot") business activities, since it appears that Webroot's Spy Sweeper product(s) may fall within the scope of one or more patent claims.

Finjan would welcome an opportunity to discuss Webroot's interest in obtaining a license to Finjan's patent portfolio. A copy of the '520 and '962 Patents have been enclosed to provide information Webroot might need to evaluate a license to these patents.

We would like to schedule a meeting sometime in the next three weeks. Please let us know your availability at your earliest convenience.

Very truly yours,

Paul J. Andre

Paul J. Andre

enclosures

Defendant's Trial Ex.
DTX - 1305
Case No. 06-369 GMS

CONFIDENTIAL

US006480962B1

(12) **United States Patent**
Touboul

(10) **Patent No.: US 6,480,962 B1**
(45) **Date of Patent: *Nov. 12, 2002**

(54) SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES

(75) Inventor: Shlomo Touboul, Kefar-Haim (IL)

(73) Assignee: Finjan Software, Ltd., Kefar-Haim (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: 09/551,302

(22) Filed: Apr. 18, 2000

Related U.S. Application Data

(63) Continuation of application No. 08/790,097, filed on Jan. 29, 1997.

(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) Int. Cl.^{7} H02H 3/05

(52) U.S. Cl. 713/200; 713/201

(58) Field of Search 713/200, 201, 713/202; 714/38, 704; 709/225, 229

(56) References Cited

U.S. PATENT DOCUMENTS

5,077,677	A	12/1991	Murphy et al.
5,359,659	A	10/1994	Rosenthal
5,361,359	A	11/1994	Tajalli et al.
5,485,409	A	1/1996	Gupta et al.
5,485,575	A	1/1996	Chess et al.
5,572,643	A	11/1996	Judson
5,606,668	A	2/1997	Shwed
5,623,600	A	4/1997	Ji et al.
5,638,446	A	6/1997	Rubin
5,692,047	A	11/1997	McManis
5,692,124	A	11/1997	Holden et al.
5,720,033	A	2/1998	Deo
5,724,425	A	3/1998	Chang et al.
5,740,248	A	4/1998	Fieres et al.
5,761,421	A	6/1998	van Hoff et al.

(List continued on next page.)

OTHER PUBLICATIONS

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pp. 21–29.

Okamoto, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013–5194, Jul. 19, 1990, Abstract and pp. 1169–1170. URL:http://iel.ihs.com:80/cgi–bin/iel_cgi?se . . . 2ehts%26ViewTemplate%3ddocview%5fb%2ehts.

IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, Nov. 15, 1995, pp. 6–7.

Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week, vol. 13, No. 29, Jul. 22, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software Ltd., Jul. 29, 1996, 1 page.

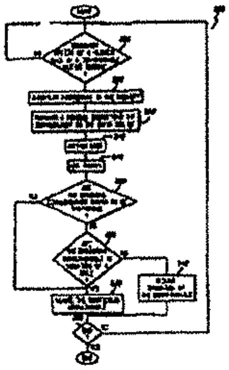
(List continued on next page.)

Primary Examiner—Dieu-Minh Le
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) ABSTRACT

A system protects a client from hostile Downloadables. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

51 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

5,765,205	A		6/1998	Breslau et al.	
5,784,459	A		7/1998	Devarakonda et al.	
5,796,952	A		8/1998	Davis et al.	
5,805,829	A		9/1998	Cohen et al.	
5,832,208	A		11/1998	Chen et al.	
5,850,559	A		12/1998	Angelo et al.	
5,859,966	A		1/1999	Hayman et al.	
5,864,683	A		1/1999	Boebert et al.	
5,892,904	A		4/1999	Atkinson et al.	
5,951,698	A		9/1999	Chen et al.	
5,956,481	A		9/1999	Walsh et al.	
5,974,549	A		10/1999	Golan	
5,983,348	A		11/1999	Ji	
6,092,194	A	*	7/2000	Touboul	713/200
6,154,844	A	*	11/2000	Touboul et al.	713/201
6,167,520	A	*	12/2000	Touboul	713/200

OTHER PUBLICATIONS

"Powerful PC Security for the New World of JAVA™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction and pp. 1–10.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, Oct. 21, 1996, 2 pages.

Company Profile "Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consultant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.

Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated Feb. 17, 1997, Printed Dec. 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pp. 1–13.

Zhang, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, vol. 30, Issue 6, Jun. 1997, pp.: 76–79.

* cited by examiner

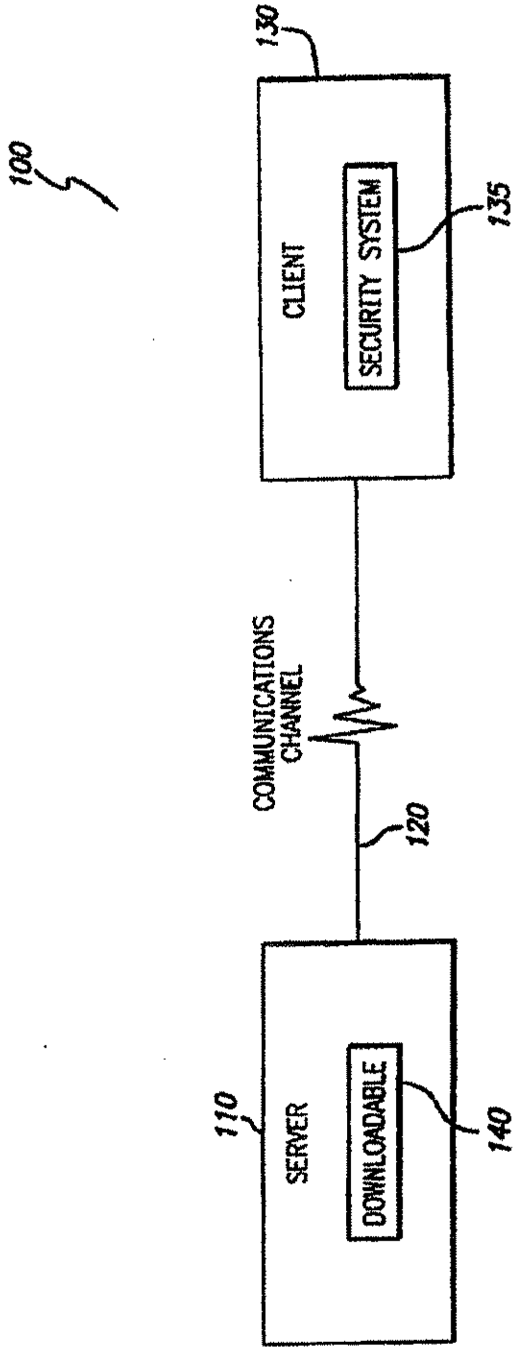

100
130
CLIENT
SECURITY SYSTEM
135
COMMUNICATIONS CHANNEL
120
110
SERVER
DOWNLOADABLE
140

FIG. 1

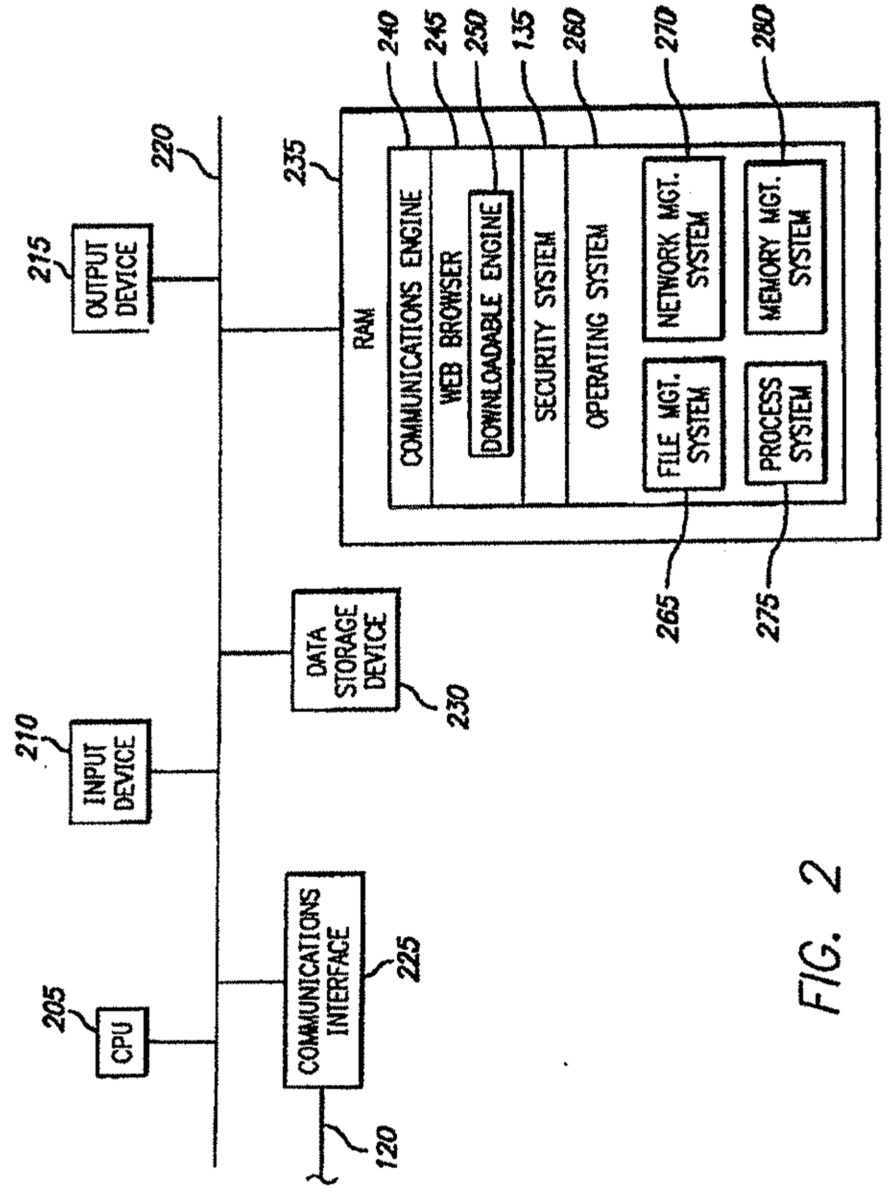

CPU
205
INPUT DEVICE
210
OUTPUT DEVICE
215
220
COMMUNICATIONS INTERFACE
225
120
DATA STORAGE DEVICE
230
RAM
235
COMMUNICATIONS ENGINE
240
WEB BROWSER
245
DOWNLOADABLE ENGINE
250
SECURITY SYSTEM
135
OPERATING SYSTEM
260
FILE MGT. SYSTEM
265
NETWORK MGT. SYSTEM
270
PROCESS SYSTEM
275
MEMORY MGT. SYSTEM
280

FIG. 2

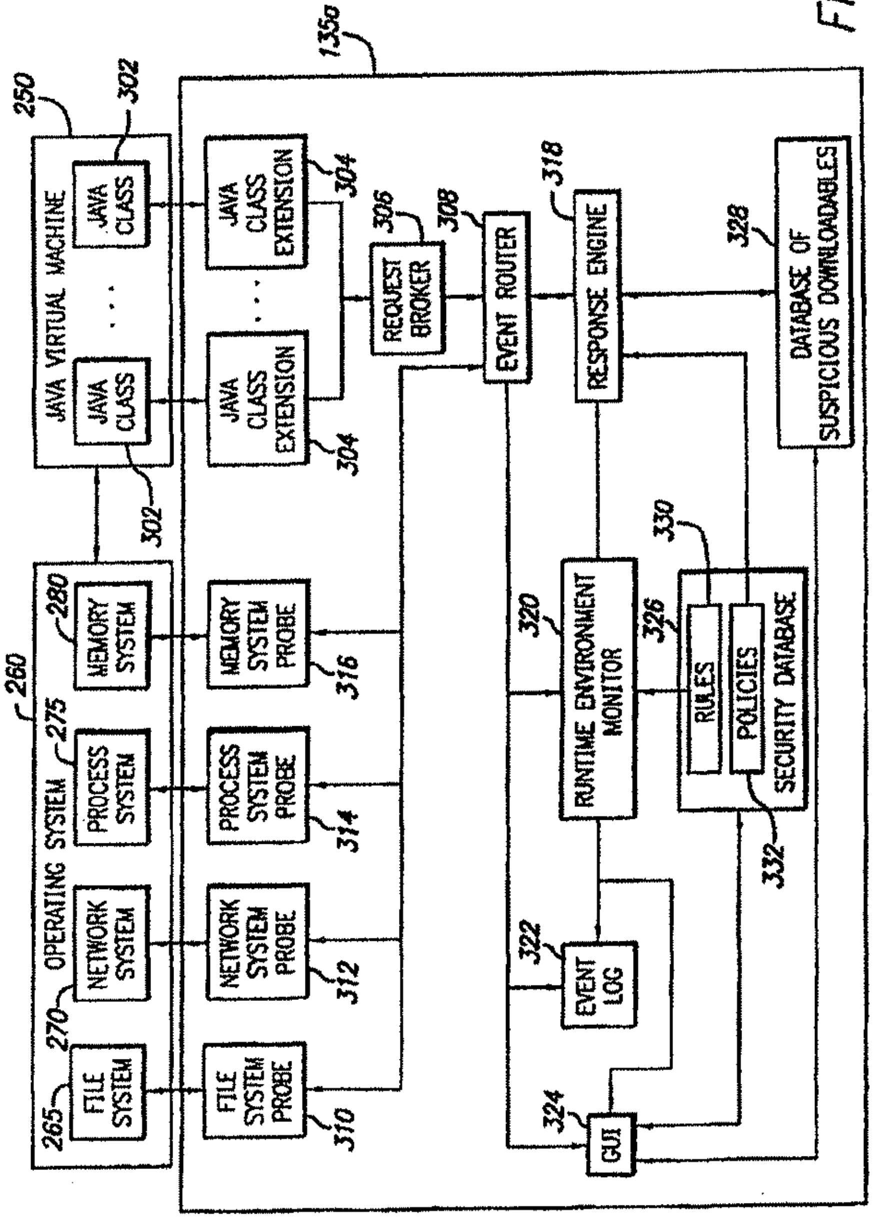

250
JAVA VIRTUAL MACHINE
JAVA CLASS
JAVA CLASS
302
302
260
OPERATING SYSTEM
265
FILE SYSTEM
270
NETWORK SYSTEM
275
PROCESS SYSTEM
280
MEMORY SYSTEM
135a
JAVA CLASS EXTENSION
JAVA CLASS EXTENSION
304
304
306
REQUEST BROKER
308
EVENT ROUTER
318
RESPONSE ENGINE
328
DATABASE OF SUSPICIOUS DOWNLOADABLES
FILE SYSTEM PROBE
310
NETWORK SYSTEM PROBE
312
PROCESS SYSTEM PROBE
314
MEMORY SYSTEM PROBE
316
320
RUNTIME ENVIRONMENT MONITOR
322
EVENT LOG
324
GUI
326
330
RULES
POLICIES
SECURITY DATABASE
332

FIG. 3

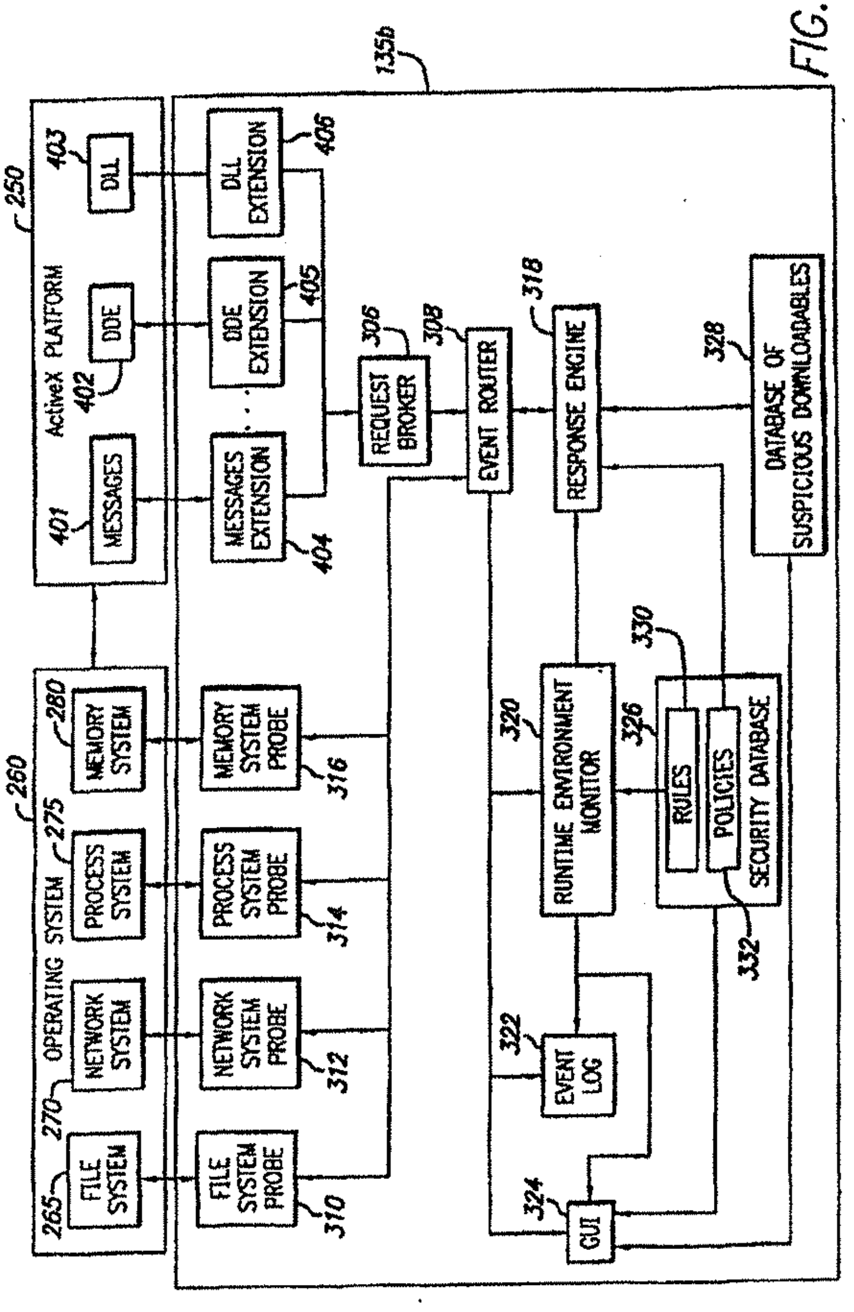

135b
250
ActiveX PLATFORM
401
MESSAGES
402
DDE
403
DLL
404
MESSAGES EXTENSION
405
DDE EXTENSION
406
DLL EXTENSION
306
REQUEST BROKER
308
EVENT ROUTER
318
RESPONSE ENGINE
328
DATABASE OF SUSPICIOUS DOWNLOADABLES
260
OPERATING SYSTEM
265
FILE SYSTEM
270
NETWORK SYSTEM
275
PROCESS SYSTEM
280
MEMORY SYSTEM
310
FILE SYSTEM PROBE
312
NETWORK SYSTEM PROBE
314
PROCESS SYSTEM PROBE
316
MEMORY SYSTEM PROBE
320
RUNTIME ENVIRONMENT MONITOR
322
EVENT LOG
324
GUI
326
RULES
330
POLICIES
332
SECURITY DATABASE

FIG. 4

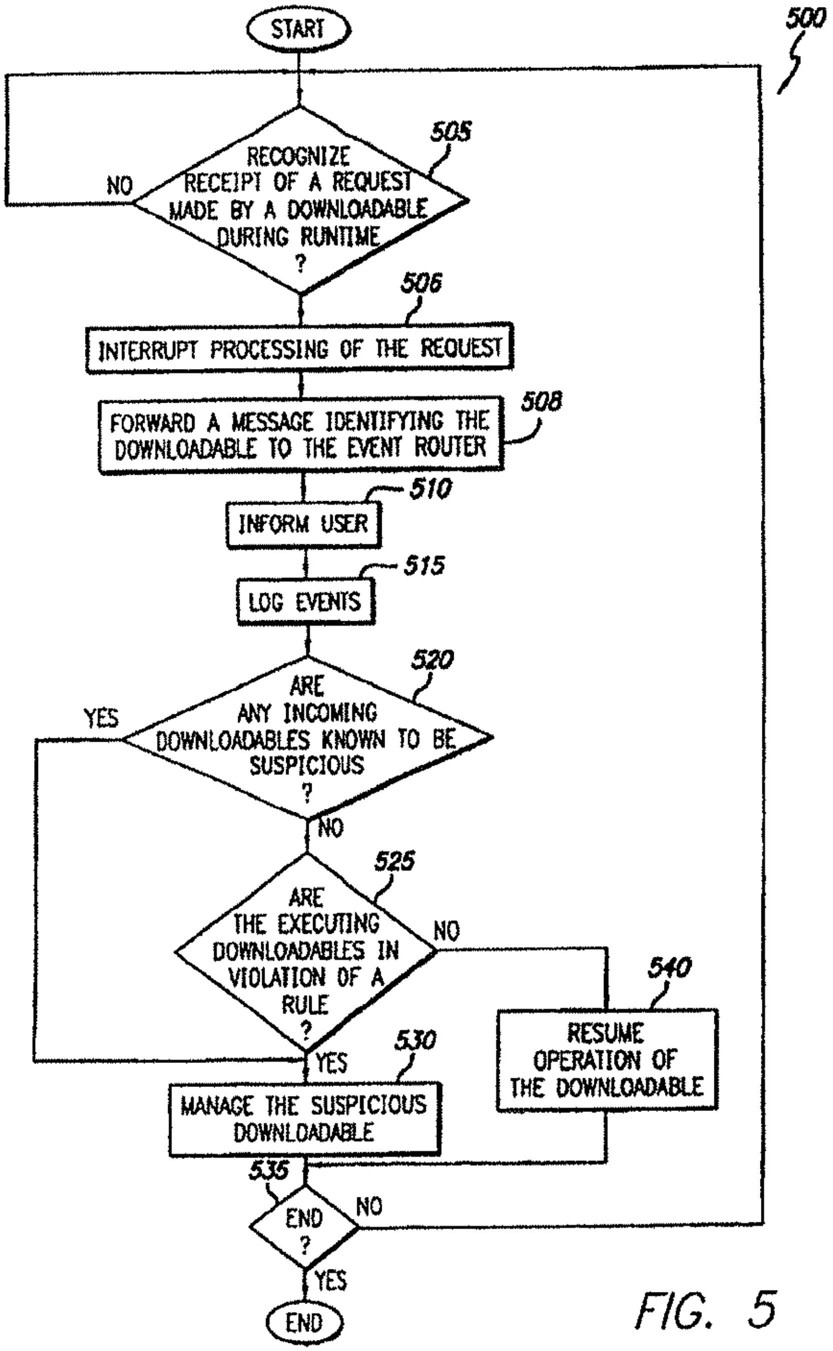

500
START
RECOGNIZE RECEIPT OF A REQUEST MADE BY A DOWNLOADABLE DURING RUNTIME ?
505
NO
506
INTERRUPT PROCESSING OF THE REQUEST
FORWARD A MESSAGE IDENTIFYING THE DOWNLOADABLE TO THE EVENT ROUTER
508
510
INFORM USER
515
LOG EVENTS
520
ARE ANY INCOMING DOWNLOADABLES KNOWN TO BE SUSPICIOUS ?
YES
NO
525
ARE THE EXECUTING DOWNLOADABLES IN VIOLATION OF A RULE ?
NO
YES
540
RESUME OPERATION OF THE DOWNLOADABLE
530
MANAGE THE SUSPICIOUS DOWNLOADABLE
535
END ?
NO
YES
END

FIG. 5

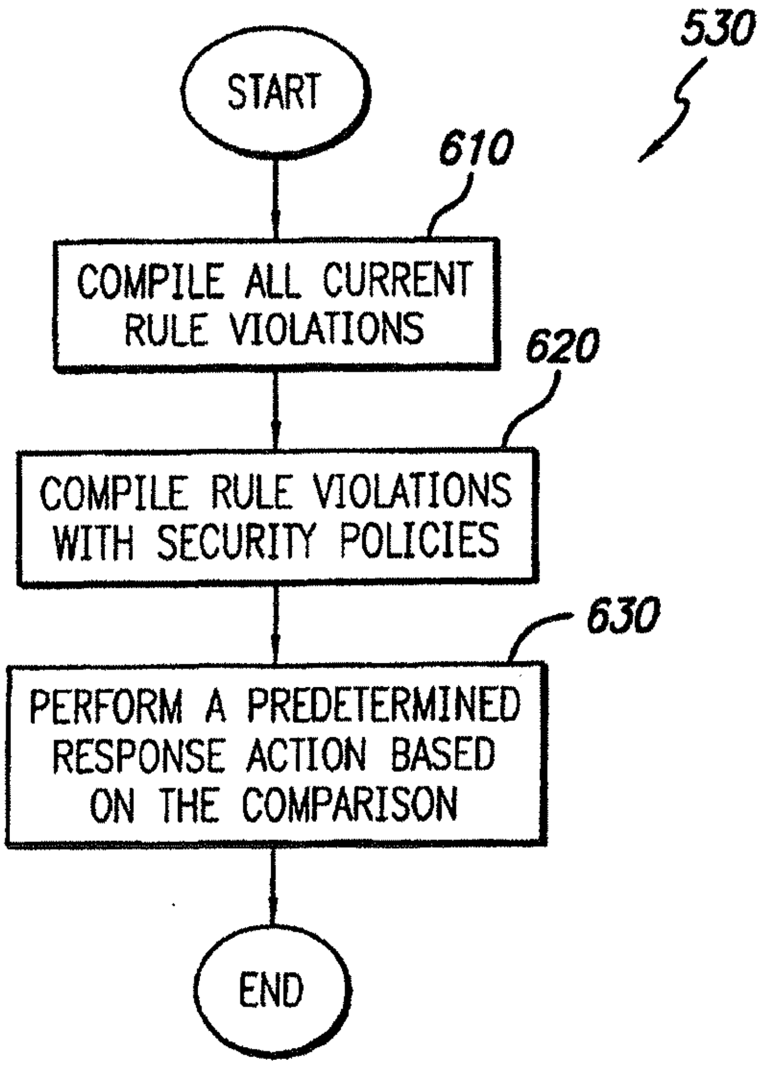

530
START
610
COMPILE ALL CURRENT RULE VIOLATIONS
620
COMPILE RULE VIOLATIONS WITH SECURITY POLICIES
630
PERFORM A PREDETERMINED RESPONSE ACTION BASED ON THE COMPARISON
END

FIG. 6

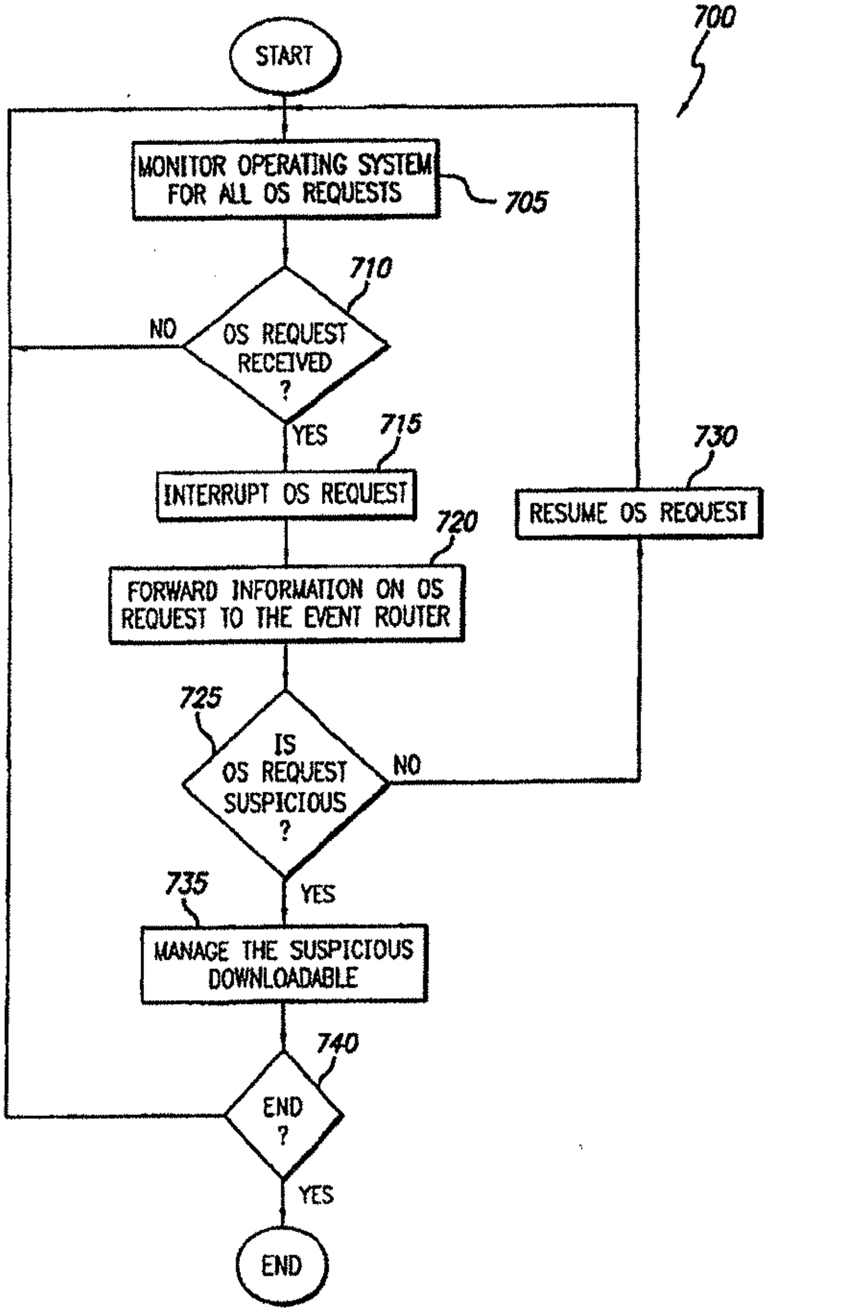

700
START
MONITOR OPERATING SYSTEM FOR ALL OS REQUESTS
705
710
NO
OS REQUEST RECEIVED ?
YES
715
INTERRUPT OS REQUEST
730
RESUME OS REQUEST
720
FORWARD INFORMATION ON OS REQUEST TO THE EVENT ROUTER
725
IS OS REQUEST SUSPICIOUS ?
NO
735
YES
MANAGE THE SUSPICIOUS DOWNLOADABLE
740
END ?
YES
END

FIG. 7

SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to co-pending provisional patent application filed on Nov. 8, 1996, entitled "System and Method for Protecting a Computer from Hostile Downloadables," Ser. No. 60/030,639, by inventor Shlomo Touboul, and is a continuation of U.S. patent application filed on Jan. 29, 1997, entitled "System and Method for Protecting a Computer During Runtime From Hostile Downloadbales," Ser. No. 08/790,097, by inventor Shlomo Touboul, which subject matters are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for protecting clients from hostile Downloadables.

2. Description of the Background Art

The Internet currently interconnects about 100,000 individual computer networks and several million computers. Because it is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

In response to the widespread generation and distribution of computer viruses, programmers continue to design and update security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are typically not configured to recognize computer viruses which have been attached to or masked as harmless Downloadables (i.e., applets). A Downloadable is a small executable or interpretable application program which is downloaded from a source computer and run on a destination computer. A Downloadable is used in a distributed environment such as in the Java™ distributed environment produced by Sun Microsystems or in the ActiveX™ distributed environment produced by Microsoft Corporation.

Hackers have developed hostile Downloadables designed to penetrate security holes in Downloadable interpreters. In response, Sun Microsystems, Inc. has developed a method of restricting Downloadable access to resources (file system resources, operating system resources, etc.) on the destination computer, which effectively limits Downloadable functionality at the Java™ interpreter. Sun Microsystems, Inc. has also provided access control management for basing Downloadable-accessible resources on Downloadable type. However, the above approaches are difficult for the ordinary web surfer to manage, severely limit Java™ performance and functionality, and insufficiently protect the destination computer.

Other security system designers are currently considering digital signature registration stamp techniques, wherein, before a web browser will execute a Downloadable, the Downloadable must possess a digital signature registration stamp. Although a digital signature registration stamp will diminish the threat of Downloadables being intercepted, exchanged or corrupted, this approach only partially addresses the problem. This method does not stop a hostile Downloadable from being stamped with a digital signature, and a digital signature does not guarantee that a Downloadable is harmless. Therefore, a system and method are needed for protecting clients from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a client from hostile Downloadables. The system includes security rules defining suspicious actions such as WRITE operations to a system configuration file, overuse of system memory, overuse of system processor time, etc. and security policies defining the appropriate responsive actions to rule violations such as terminating the applet, limiting the memory or processor time available to the applet, etc. The system includes an interface, such as Java™ class extensions and operating system probes, for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing the violation-based responsive action.

The present invention further provides a method for protecting a client from hostile Downloadables. The method includes the steps of recognizing a request made by a Downloadable during runtime, interrupting processing of the request, comparing information pertaining to the Downloadable against a predetermined security policy, recording all rule violations in a log, and performing a predetermined responsive action based on the comparison.

It will be appreciated that the system and method of the present invention use at least three hierarchical levels of security. A first level examines the incoming Downloadables against known suspicious Downloadables. A second level examines runtime events. A third level examines the Downloadables operating system requests against predetermined suspicious actions. Thus, the system and method of the invention are better able to locate hostile operations before client resources are damaged.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a network system in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of the client;

FIG. 3 is a block diagram illustrating details of a security system;

FIG. 4 is a block diagram illustrating details of an alternative security system;

FIG. 5 is a flowchart illustrating a method for protecting a client from suspicious Downloadables;

FIG. 6 is a flowchart illustrating the method for managing a suspicious Downloadable; and

FIG. 7 is a flowchart illustrating a supplementary method for protecting a client from suspicious Downloadables.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating a network system 100 in accordance with the present invention. Network system 100 includes a server 110 coupled to a communications channel 120, e.g., an Internet or an Intranet. The communications channel 120 is in turn coupled to a client 130, e.g., an individual computer, a network computer, a kiosk workstation, etc., which includes a security system

135 for protecting the client 130 from hostile (i.e., will adversely effect the operational characteristics of the client 130) or suspicious (i.e., potentially hostile) downloadables.

Server 110 forwards a Downloadable 140 across the communications channel 120 to the client 130. During runtime, the security system 135 examines each Downloadable 140 and the actions of each Downloadable 140 to monitor for hostile or suspicious actions.

FIG. 2 is a block diagram illustrating details of a client 130, which includes a Central Processing Unit (CPU) 205, such as a Motorola Power PC® microprocessor or an Intel Pentium® microprocessor, coupled to a signal bus 220. The client 130 further includes an input device 210 such as a keyboard and mouse, an output device 215 such as a Cathode Ray Tube (CRT) display, a data storage device 230 such as Read Only Memory (ROM) or magnetic disk, and a Random-Access Memory (RAM) 235, each being coupled to signal bus 220. A communications interface 225 is coupled between the communications channel 120 and the signal bus 220.

An operating system 260 controls processing by CPU 205, and is typically stored in data storage device 230 and loaded into RAM 235 for execution. The operating system 260 includes a file management system 265, a network management system 270, a process system 275 for controlling CPU 205, and a memory management system 280 for controlling memory use and allocation. A communications engine 240 generates and transfers message packets to and from the communications channel 140 via the communications interface 225, and may also be stored in data storage device 230 and loaded into RAM 235 for execution.

The client 130 further includes a web browser 245, such as the Netscape™ web browser produced by the Netscape Corporation, the Internet Explorer™ web browser produced by the Microsoft Corporation, or the Java™ Developers Kit 1.0 web browser produced by Sun Microsystems, Inc., for communicating via the communications channel 120. The web browser 245 includes a Downloadable engine 250 for managing and executing received Downloadables 140.

The client 130 further includes the security system 135 as described with reference to FIG. 1. The security system 135 may be stored in data storage device 230 and loaded into RAM 235 for execution. During runtime, the security system 135 intercepts and examines Downloadables 140 and the actions of Downloadables 140 to monitor for hostile or suspicious actions. If the security system 135 recognizes a suspicious Downloadable 140 or a suspicious request, then the security system 135 can perform an appropriate responsive action such as terminating execution of the Downloadable 140.

FIG. 3 is a block diagram illustrating details of the security system 135a, which is a first embodiment of security system 135 of FIG. 2 when operating in conjunction with a Java™ virtual machine 250 (i.e., the Downloadable engine 250) that includes conventional Java™ classes 302. Each of the Java™ classes 302 performs a particular service such as loading applets, managing the network, managing file access, etc. Although applets are typically described with reference to the Java™ distributed environment, applets herein correspond to all downloadable executable or interpretable programs for use in any distributed environment such as in the ActiveX™ distributed environment.

Examples of Java™ classes used in Netscape Navigator™ include AppletSecurity.class, EmbeddedAppletFrame.class:, AppletClassLoader.class, MozillaAppletContext.class, ServerSocket.class, SecurityException.class and

SecurityManager.class, etc. Examples of Java™ classes used in Internet Explorer™ include AppletSecurity.class, BrowserAppletFrame.class, AppletClassLoader.class, ServerSocket.class, SecurityException.class and SecurityManager.class, etc. Other classes may include Broker.class, BCInterface.class, SocketConnection.class, queueManager.class, BrowserExtension.class, Message.class, MemoryMeter.class and AppletDescription.class.

The security system 135a includes Java™ class extensions 304, wherein each extension 304 manages a respective one of the Java™ classes 302. When a new applet requests the service of a Java class 302, the corresponding Java™ class extension 304 interrupts the request and generates a message to notify the request broker 306 of the Downloadable's request. The request broker 306 uses TCP/IP message passing protocol to forward the message to the event router 308.

The security system 135a further includes operating system probes 310, 312, 314 and 316. More particularly, a file management system probe 310 recognizes applet instructions sent to the file system 265 of operating system 260, a network system probe 312 recognizes applet instructions set to the network management system 270 of operating system 260, a process system probe 314 recognizes applet instructions sent to the process system 275 of operating system 260, and a memory management system probe 316 recognizes applet instructions sent to the memory system 280 of operating system 260. When any of the probes 310–316 recognizes an applet instruction, the recognizing probe 310–316 sends a message to inform the event router 308.

Upon receipt of a message, the event router 308 accordingly forwards the message to a Graphical User Interface (GUI) 324 for notifying the user of the request, to an event log 322 for recording the message for subsequent analysis, and to a runtime environment monitor 320 for determining whether the request violates a security rule 330 stored in a security database 326. Security rules 330 include a list of computer operations which are deemed suspicious. Suspicious operations may include READ/WRITE operations to a system configuration file, READ/WRITE operations to a document containing trade secrets, overuse of system memory, overuse of system processor time, too many applets running concurrently, or too many images being displayed concurrently. For example, the runtime environment monitor 320 may determine that a security rule 330 has been violated when it determines that an applet uses more than two megabytes of RAM 235 or when the Java™ virtual machine 250 runs more than five applets concurrently.

Upon recognition of a security rule 330 violation, the runtime environment monitor 320 records the violation with the event log 322, informs the user of the violation via the GUI 324 and forwards a message to inform the response engine 318 of the violation. The response engine 318 analyzes security policies 332 stored in the security database 326 to determine the appropriate responsive action to the rule 330 violation. Appropriate responsive actions may include terminating the applet, limiting the memory or processor time available to the applet, etc. For example, the response engine 318 may determine that a security policy 332 dictates that when more than five applets are executed concurrently, operation of the applet using the greatest amount of RAM 235 should be terminated. Further, a security policy 332 may dictate that when an applet or a combination of applets violates a security policy 332, the response engine 318 must add information pertaining to the applet or applets to the suspicious Downloadables database

328. Thus, when the applet or applets are encountered again, the response engine 318 can stop them earlier.

The GUI 324 enables a user to add or modify the rules 330 of the security database 326, the policies 332 of the security database 326 and the suspicious applets of the suspicious Downloadables database 328. For example, a user can use the GUI 324 to add to the suspicious Downloadables database 328 applets generally known to be hostile, applets deemed to be hostile by the other clients 130 (not shown), applets deemed to be hostile by network MIS managers, etc. Further, a user can use the GUI 324 to add to the rules 330 actions generally known to be hostile, actions deemed to be hostile by network MIS managers, etc.

It will be appreciated that the embodiment illustrated in FIG. 3 includes three levels of security. The first level examines the incoming Downloadables 140 against known suspicious Downloadables. The second level examines the Downloadables'access to the Java™ classes 302. The third level examines the Downloadables requests to the operating system 260. Thus, the security system 135*a* is better apt to locate a hostile operation before an operation damages client 130 resources.

FIG. 4 is a block diagram illustrating details of a security system 135*b*, which is a second embodiment of security system 135 when operating in conjunction with the ActiveX™ platform (i.e., the Downloadable engine 250) which uses message 401 calls, Dynamic-Data-Exchange (DDE) 402 calls and Dynamically-Linked-Library (DLL) 403 calls. Thus, instead of having Java™ class extensions 304, the security system 135 has a messages extension 401 for recognizing message 401 calls, a DDE extension 405 for recognizing DDE 402 calls and a DLL extension 406 for recognizing DLL calls. Upon recognition of a call, each of the messages extension 404, the DDE extension 405 and the DLL extension 406 send a message to inform the request broker 306. The request broker 306 and the remaining elements operate similarly to the elements described with reference to FIG. 3.

FIG. 5 is a flowchart illustrating a method 500 for protecting a client 130 from hostile and suspicious Downloadables 140. Method 500 begins with the extensions 304, 404, 405 or 406 in step 505 waiting to recognize the receipt of a request made by a Downloadable 140. Upon recognition of a request, the recognizing extension 304, 404, 405 or 406 in step 506 interrupts processing of the request and in step 508 generates and forwards a message identifying the incoming Downloadable 140 to the request broker 306, which forwards the message to the event router 308.

The event router 308 in step 510 forwards the message to the GUI 324 for informing the user and in step 515 to the event log 322 for recording the event. Further, the event router 308 in step 520 determines whether any of the incoming Downloadables 140 either alone or in combination are known or previously determined to be suspicious. If so, then method 500 jumps to step 530. Otherwise, the runtime environment monitor 320 and the response engine 318 in step 525 determine whether any of the executing Downloadables 140 either alone or in combination violate a security rule 330 stored in the security database 332.

If a rule 330 has been violated, then the response engine 318 in step 530 manages the suspicious Downloadable 140. Step 530 is described in greater detail with reference to FIG. 6. Otherwise, if a policy has not been violated, then response engine 318 in step 540 resumes operation of the Downloadable 140. In step 535, a determination is made whether to end method 500. For example, if the user disconnects the

client 130 from the server 110, method 500 ends. If a request to end is made, then method 500 ends. Otherwise, method 500 returns to step 505.

FIG. 6 is a flowchart illustrating details of step 530. Since multiple rule 330 violations may amount to a more serious violation and thus require a stricter response by the response engine 318, step 530 begins with the response engine 318 in step 610 compiling all rule 330 violations currently occurring. The response engine 318 in step 620 compares the compiled rule 330 violations with the security policies 332 to determine the appropriate responsive action for managing the suspicious Downloadable 140 or Downloadables 140, and in step 630 the response engine 318 performs a predetermined responsive action. Predetermined responsive actions may include sending a message via the GUI 324 to inform the user, recording the message in the event log 322, stopping execution of a suspicious Downloadable 140, storing a Downloadable 140 or combination of Downloadables 140 in the suspicious Downloadable database 328, limiting memory available to the Downloadable 140, limiting processor time available to the Downloadable 140, etc.

FIG. 7 is a flowchart illustrating a supplementary method 700 for protecting a client 130 from suspicious Downloadables 140. Method 700 begins with operating system probes 310, 312, 314 and 316 in step 705 monitoring the operating system 260 for Operating System (OS) requests from Downloadables 140. As illustrated by step 710, when one of the probes 310–316 recognizes receipt of an OS request, the recognizing probe 310–316 in step 715 interrupts the request and in step 720 forwards a message to inform the event router 308.

The event router 308 in step 725 routes the information to each of the components of the security engine 135 as described with reference to FIG. 5. That is, the event router 308 forwards the information to the GUI 324 for informing the user, to the event log 322 for recordation and to the runtime environment monitor 320 for determining if the OS request violates a rule 330. The response engine 318 compares the OS request alone or in combination with other violations against security policies 332 to determine the appropriate responsive actions. It will be appreciated that, based on the security policies 332, the response engine 318 may determine that an OS request violation in combination with other OS request violations, in combination with rule 330 violations, or in combination with both other OS request violations and rule 330 violations merits a stricter responsive action.

If the OS request does not violate a security rule 330, then the response engine 318 in step 730 instructs the operating system 260 via the recognizing probe 310–316 to resume operation of the OS request. Otherwise, if the OS request violates a security rule 330, then the response engine 318 in step 730 manages the suspicious Downloadable by performing the appropriate predetermined responsive actions as described with reference to FIGS. 5 and 6. In step 740, a determination is made whether to end method 700. If a request to end the method is made, then method 700 ends. Otherwise, method 700 returns to step 705.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising:

monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison.

2. The method of claim 1, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

3. The method of claim 2,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

4. The method of claim 2,

wherein the Downloadable engine includes an ActiveX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

5. The method of claim 1, further comprising determining whether information pertaining to the Downloadable violates a security rule.

6. The method of claim 5, further comprising determining whether violation of the security rule violates the security policy.

7. The method of claim 1, further comprising:

comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

8. The method of claim 1, wherein the predetermined responsive action includes storing results of the comparison in an event log.

9. The method of claim 1, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

10. The method of claim 1, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

11. The method of claim 1, wherein the predetermined responsive action includes discarding the Downloadable.

12. A system, comprising:

a security policy;

a plurality of operating system interfaces operating substantially in parallel, each interface for recognizing a runtime event in a subsystem of the operating system caused from a request made by a Downloadable;

a first comparator coupled to the interfaces for comparing information pertaining to the received Downloadable with the security policy; and

a response engine coupled to the first comparator for performing a predetermined responsive action based on the comparison with the security policy.

13. The system of claim 12, wherein the interfaces include a Java™ class extension for monitoring a Java™ class in a Java™ virtual machine for receipt of a request.

14. The system of claim 12, wherein the interfaces include an ActiveX™ extension for monitoring a message engine, a dynamic-data-exchange and a dynamically-linked library in an ActiveX™ environment for receipt of a request.

15. The system of claim 12, further comprising

a security rule; and

a second comparator, coupled to the interfaces and to the response engine, for determining whether information pertaining to the Downloadable violates the security rule.

16. The system of claim 15, wherein the first comparator determines whether violation of the security rule violates the security policy.

17. The system of claim 12, further comprising

a predetermined suspicious Downloadable; and

a second comparator coupled to the interfaces for comparing information pertaining to the Downloadable with information pertaining to the predetermined suspicious Downloadable;

wherein the response engine is further coupled to the second comparator and performs the responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

18. The system of claim 12, further comprising an event log coupled to the first comparator for storing results of the comparison.

19. The system of claim 12, further comprising a user interface coupled to the first comparator.

20. The system of claim 12, further comprising a suspicious Downloadable database for storing information on known and previously-deemed suspicious Downloadables.

21. The system of claim 12, wherein the predetermined suspicious action includes discarding the Downloadable.

22. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison.

23. The system of claim 22, wherein the means for monitoring the operating system includes means for monitoring a request sent to a Downloadable engine.

24. The system of claim 23,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein the means for monitoring the operating system includes means for monitoring each Java™ class for receipt of the request.

25. The system of claim 23,

wherein the Downloadable engine includes an ActiveX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein the means for monitoring the operating system includes means for monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

26. The system of claim 22, further comprising means for determining whether information pertaining to the Downloadable violates a security rule.

27. The system of claim 26, further comprising means for determining whether violation of the security rule violates the security policy.

28. The method of claim 22, further comprising:

means for comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

means for performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

29. The system of claim 22, wherein the predetermined responsive action includes storing results of the comparison in an event log.

30. The system of claim 22, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

31. The system of claim 22, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

32. The system of claim 22, wherein the predetermined responsive action includes discarding the Downloadable.

33. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring substantially in parallel a plurality of subsystems of the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison.

34. The medium of claim 33, wherein monitoring the operating system includes monitoring a request sent to a Downloadable engine.

35. The medium of claim 33,

wherein the Downloadable engine includes a Java™ virtual machine having Java™ classes; and

wherein monitoring the operating system includes monitoring each Java™ class for receipt of the request.

36. The medium of claim 35,

wherein the Downloadable engine includes an AppletX™ platform having a message engine, a dynamic-data-exchange and a dynamically-linked library; and

wherein monitoring the operating system includes monitoring the message engine, the dynamic-data-exchange and the dynamically-linked library for receipt of the request.

37. The medium of claim 33, further comprising determining whether information pertaining to the Downloadable violates a security rule.

38. The medium of claim 37, further comprising determining whether violation of the security rule violates the security policy.

39. The medium of claim 33, further comprising:

comparing information pertaining to the Downloadable with information pertaining to a predetermined suspicious Downloadable; and

performing a predetermined responsive action based on the comparison with the information pertaining to the predetermined suspicious Downloadable.

40. The medium of claim 33, wherein the predetermined responsive action includes storing results of the comparison in an event log.

41. The medium of claim 33, wherein the predetermined responsive action includes informing the user when the security policy has been violated.

42. The medium of claim 33, wherein the predetermined responsive action includes storing information on the Downloadable in a suspicious Downloadable database.

43. The medium of claim 33, wherein the predetermined responsive action includes discarding the Downloadable.

44. The system of claim 1, wherein each subsystem includes one of a file system, network system, process system or memory system.

45. The system of claim 12, wherein each subsystem includes one of a file system, network system, process system or memory system.

46. The system of claim 22, wherein each subsystem includes one of a file system, network system, process system or memory system.

47. The system of claim 33, wherein each subsystem includes one of a file system, network system, process system or memory system.

48. A method, comprising:

intercepting, by an operating system probe associated with an operating system function, an operating system call being issued by a downloadable to an operating system and associated with the operating system function;

comparing, by a runtime environment monitor, the operating system call against a predetermined security policy before allowing the operating system to process the operating system call;

blocking, by a response engine, operating system calls that are forbidden according to the security policy; and

allowing, by the response engine, operating system calls that are permitted according to the security policy.

49. The method of claim 48, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

50. A system, comprising:

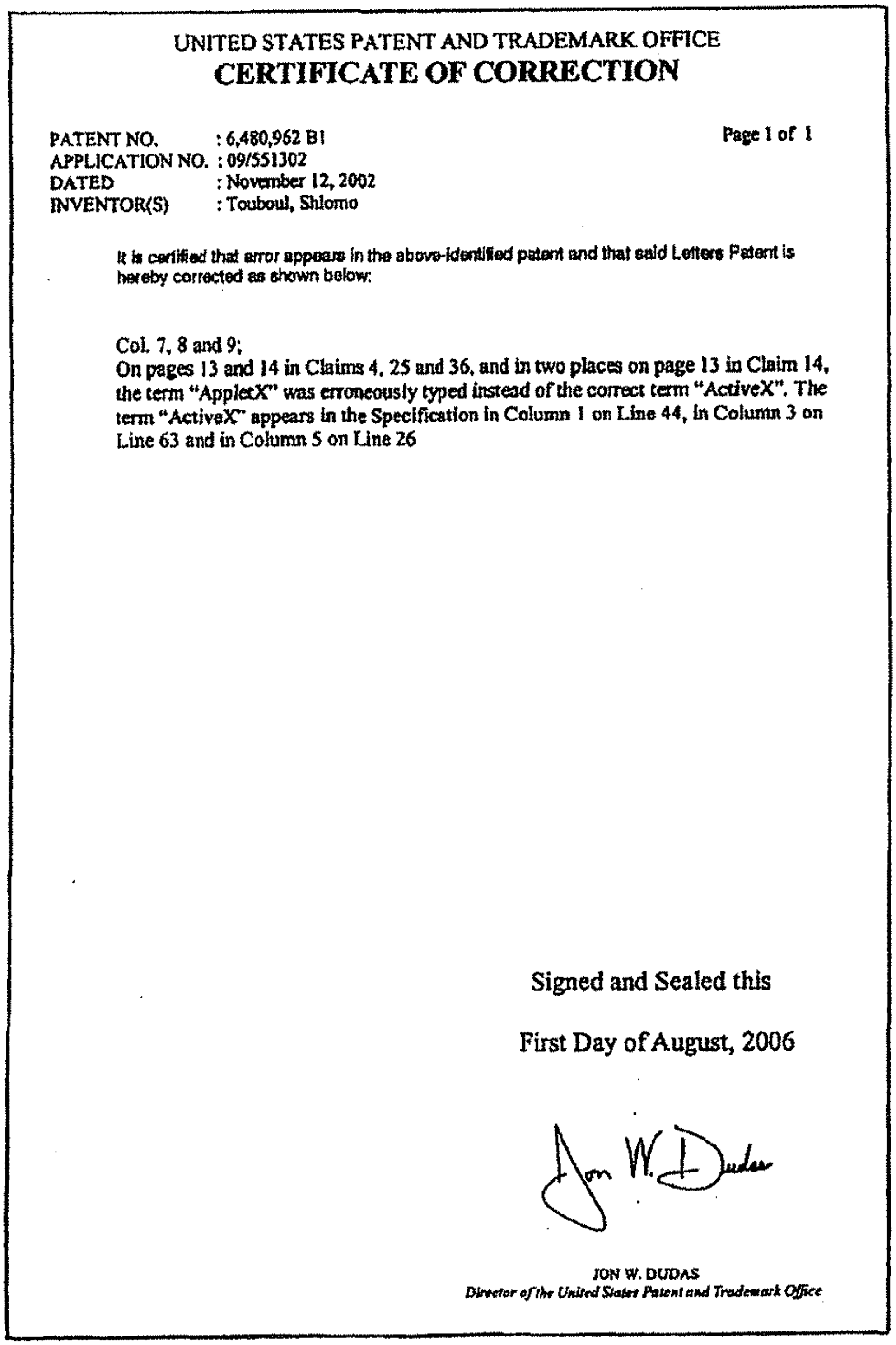
an operating system probe associated with an operating system function for intercepting an operating system call being issued by a downloadable to an operating system and associated with the operating system function;

a runtime environment monitor for comparing the operating system call against a predetermined security policy before allowing the operating system to process the operating system call; and

a response engine for blocking operating system calls that are forbidden according to the security policy, and for allowing operating system calls that are permitted according to the security policy.

51. The system of claim 50, wherein the Downloadable is one of a Java component, an ActiveX control, executable code, or interpretable code.

* * * * *



UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,480,962 B1
APPLICATION NO. : 09/551302
DATED : November 12, 2002
INVENTOR(S) : Touboul, Shlomo

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Col. 7, 8 and 9;
On pages 13 and 14 in Claims 4, 25 and 36, and in two places on page 13 in Claim 14, the term "AppletX" was erroneously typed instead of the correct term "ActiveX". The term "ActiveX" appears in the Specification in Column 1 on Line 44, in Column 3 on Line 63 and in Column 5 on Line 26

Signed and Sealed this

First Day of August, 2006

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

US006167520A

United States Patent [19]

Touboul

[11] Patent Number: 6,167,520

[45] Date of Patent: Dec. 26, 2000

[54] SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES

[75] Inventor: Shlomo Touboul, Kefar-Haim, Israel

[73] Assignee: Finjan Software, Inc., San Jose, Calif.

[21] Appl. No.: 08/790,097

[22] Filed: Jan. 29, 1997

Related U.S. Application Data

[60] Provisional application No. 60/030,639, Nov. 8, 1996.

[51] Int. Cl.^{7} G06F 11/30; H04L 9/00

[52] U.S. Cl. 713/200; 709/225

[58] Field of Search 395/186, 200.55, 395/200.59; 364/222.5, 286.4, 286.5; 326/8; 711/163; 713/200, 201; 380/4, 25

[56] References Cited

U.S. PATENT DOCUMENTS

5,077,677	12/1991	Murphy et al.	395/10
5,359,659	10/1994	Rosenthal	380/4
5,361,359	11/1994	Tajalli et al.	395/700
5,485,409	1/1996	Gupta et al.	395/186
5,485,575	1/1996	Chess et al.	395/183.14
5,572,643	11/1996	Judson	395/793
5,623,600	4/1997	Ji et al.	395/187.01
5,638,446	6/1997	Rubin	380/25
5,692,047	11/1997	McManis	380/4
5,692,124	11/1997	Holden et al.	395/187.01
5,720,033	2/1998	Deo	395/186
5,724,425	3/1998	Chang et al.	380/25
5,740,248	4/1998	Fieres et al.	380/25
5,761,421	6/1998	Van Hoff et al.	395/200.53
5,765,205	6/1998	Breslau et al.	711/203
5,784,459	7/1998	Devarakonda et al.	380/4
5,796,952	8/1998	Davis et al.	395/200.54
5,805,829	9/1998	Cohen et al.	395/200.32
5,832,208	11/1998	Chen et al.	395/187.01
5,850,559	12/1998	Angelo et al.	395/750.03
5,859,966	1/1999	Hayman et al.	395/186
5,864,683	1/1999	Boebert et al.	395/200.79
5,892,904	4/1999	Atkinson et al.	395/187.01
5,956,481	9/1999	Walsh et al.	395/186
5,983,348	11/1999	Ji	713/200

OTHER PUBLICATIONS

IBM AntiVirus User's Guide Version 2.4, p. 6–7, Nov. 1995.

Zhang, X.N., *Computer*, "Secure Code Distribution," vol. 30, Jun., 1997, pp.: 76–79.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6", Press Release of Finjan Releases SurfinShield, Oct. 21, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software, Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

"Company Profile Finjan—Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavillion 5 P5551, Nov. 18, 1996, 3 pages.

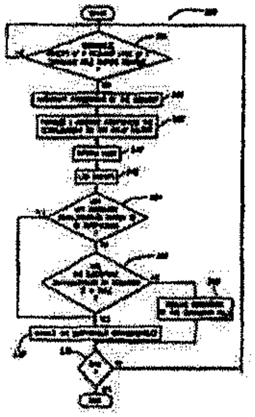
(List continued on next page.)

Primary Examiner—Dieu-Minh T. Le
Attorney, Agent, or Firm—Graham & James LLP

[57] ABSTRACT

A system and method examine execution or interpretation of a Downloadable for operations deemed suspicious or hostile, and respond accordingly. The system includes security rules defining suspicious actions and security policies defining the appropriate responsive actions to rule violations. The system includes an interface for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing a violation-based responsive action.

8 Claims, 6 Drawing Sheets



OTHER PUBLICATIONS

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

Mark LaDue, "Online Business Consultant" Article published on the Internet, Home Page, Inc. 1996, 4 pages.

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May 1990; pp. 21–27.

Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week, v13, n29, 2 pages, Jul. 22, 1996.

Microsoft Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including contents, Introduction and pp. 1–10.

Web page: http://iel.ihs.com:80/cgi–bin/iel_cgi?se . . . 2ehts%26ViewTemplate%3ddocview%5fb%2ehts, Okamoto, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013–5194, Jul. 19, 1990, Abstract and pp. 1169–1170.

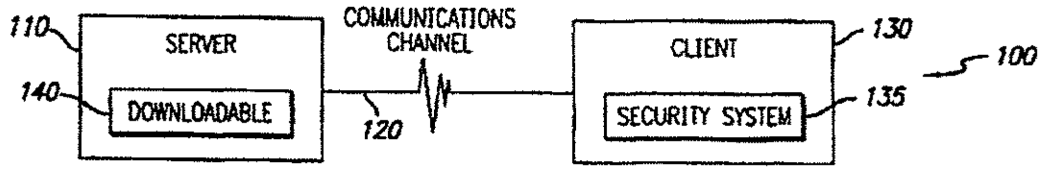

110
140
SERVER
DOWNLOADABLE
COMMUNICATIONS CHANNEL
120
CLIENT
SECURITY SYSTEM
130
135
100

FIG. 1

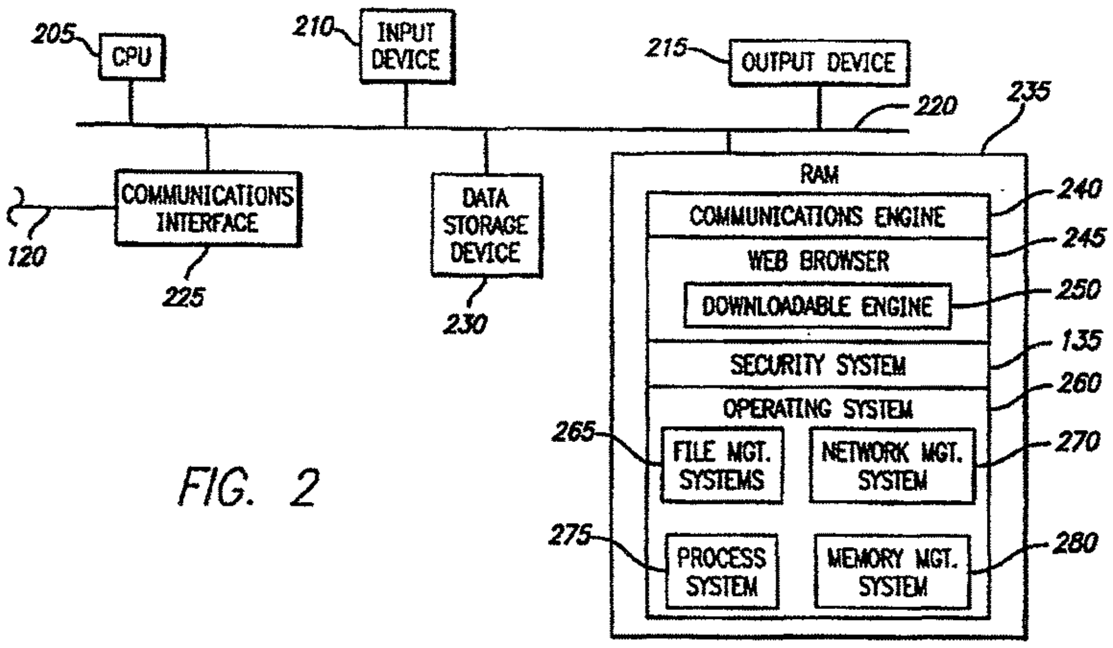

205
CPU
210
INPUT DEVICE
215
OUTPUT DEVICE
220
235
COMMUNICATIONS INTERFACE
120
225
DATA STORAGE DEVICE
230
RAM
COMMUNICATIONS ENGINE
240
WEB BROWSER
245
DOWNLOADABLE ENGINE
250
SECURITY SYSTEM
135
OPERATING SYSTEM
260
265
FILE MGT. SYSTEMS
NETWORK MGT. SYSTEM
270
275
PROCESS SYSTEM
MEMORY MGT. SYSTEM
280

FIG. 2

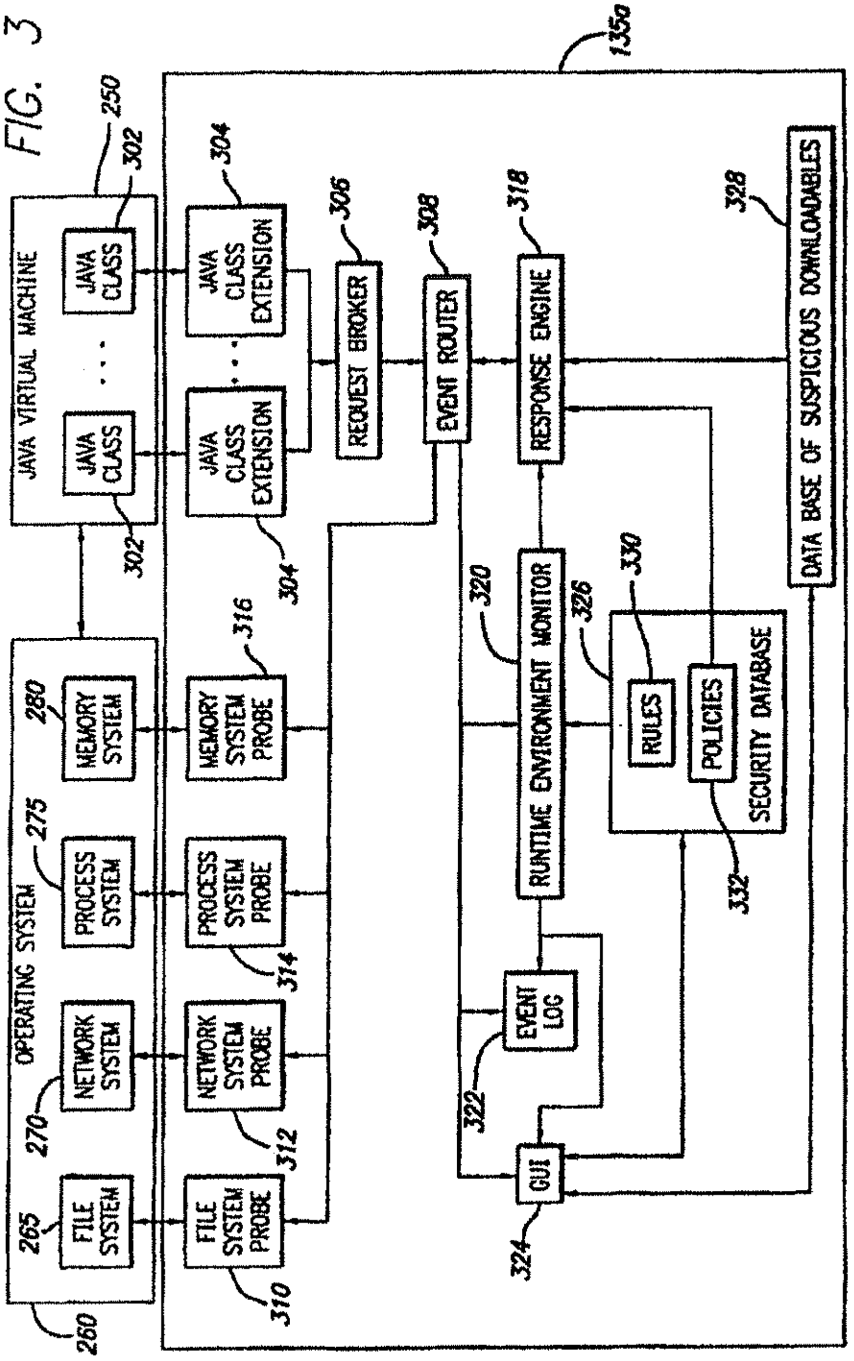


FIG. 3
JAVA VIRTUAL MACHINE
250
JAVA CLASS
302
JAVA CLASS
302
OPERATING SYSTEM
260
FILE SYSTEM
265
NETWORK SYSTEM
270
PROCESS SYSTEM
275
MEMORY SYSTEM
280
135a
JAVA CLASS EXTENSION
304
JAVA CLASS EXTENSION
304
REQUEST BROKER
306
EVENT ROUTER
308
FILE SYSTEM PROBE
310
NETWORK SYSTEM PROBE
312
PROCESS SYSTEM PROBE
314
MEMORY SYSTEM PROBE
316
RESPONSE ENGINE
318
RUNTIME ENVIRONMENT MONITOR
320
EVENT LOG
322
GUI
324
SECURITY DATABASE
326
RULES
330
POLICIES
332
DATA BASE OF SUSPICIOUS DOWNLOADABLES
328

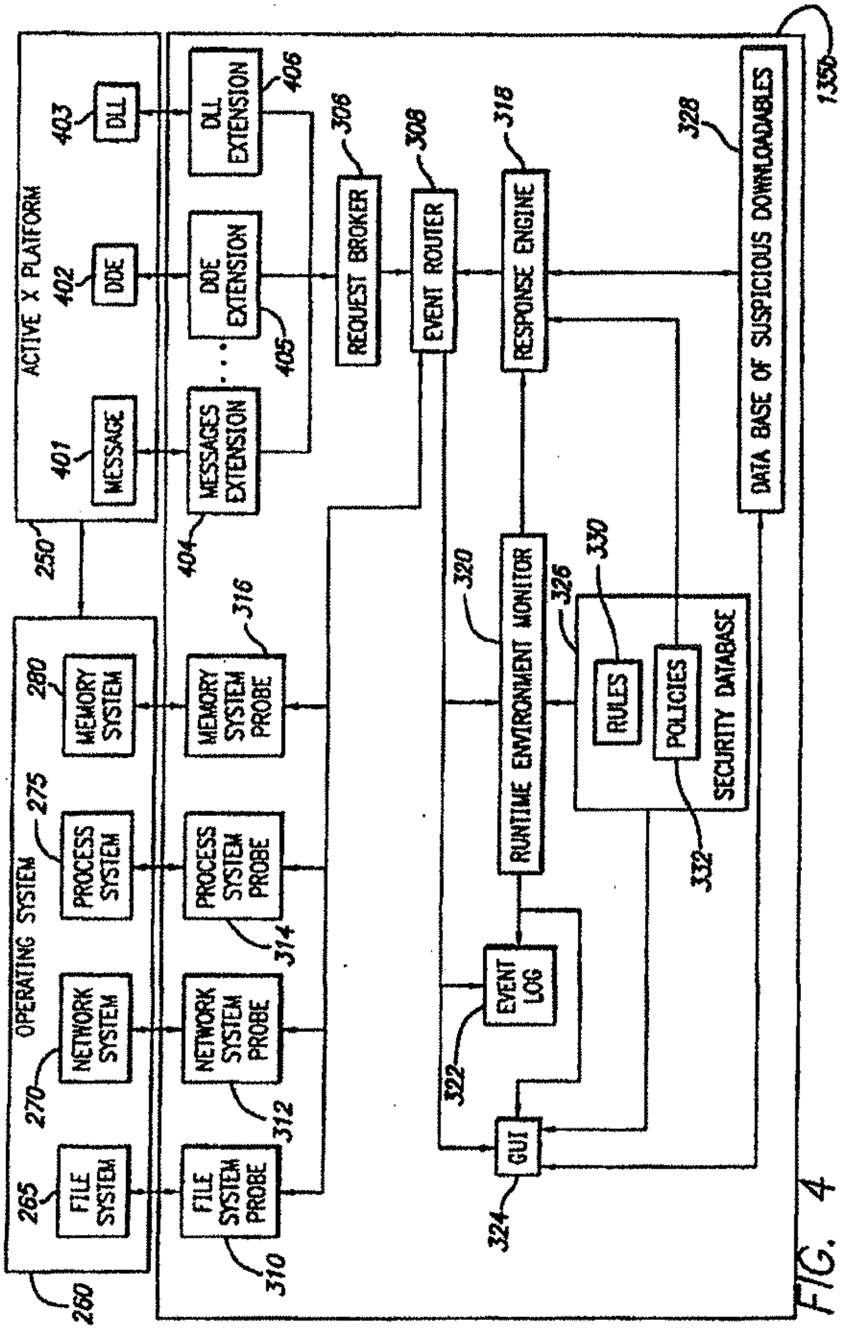

ACTIVE X PLATFORM
250
401
MESSAGE
402
DDE
403
DLL
404
MESSAGES EXTENSION
405
DDE EXTENSION
406
DLL EXTENSION
306
REQUEST BROKER
308
EVENT ROUTER
318
RESPONSE ENGINE
328
DATA BASE OF SUSPICIOUS DOWNLOADABLES
1350
OPERATING SYSTEM
260
265
FILE SYSTEM
270
NETWORK SYSTEM
275
PROCESS SYSTEM
280
MEMORY SYSTEM
310
FILE SYSTEM PROBE
312
NETWORK SYSTEM PROBE
314
PROCESS SYSTEM PROBE
316
MEMORY SYSTEM PROBE
320
RUNTIME ENVIRONMENT MONITOR
326
330
RULES
POLICIES
332
SECURITY DATABASE
322
EVENT LOG
324
GUI

FIG. 4

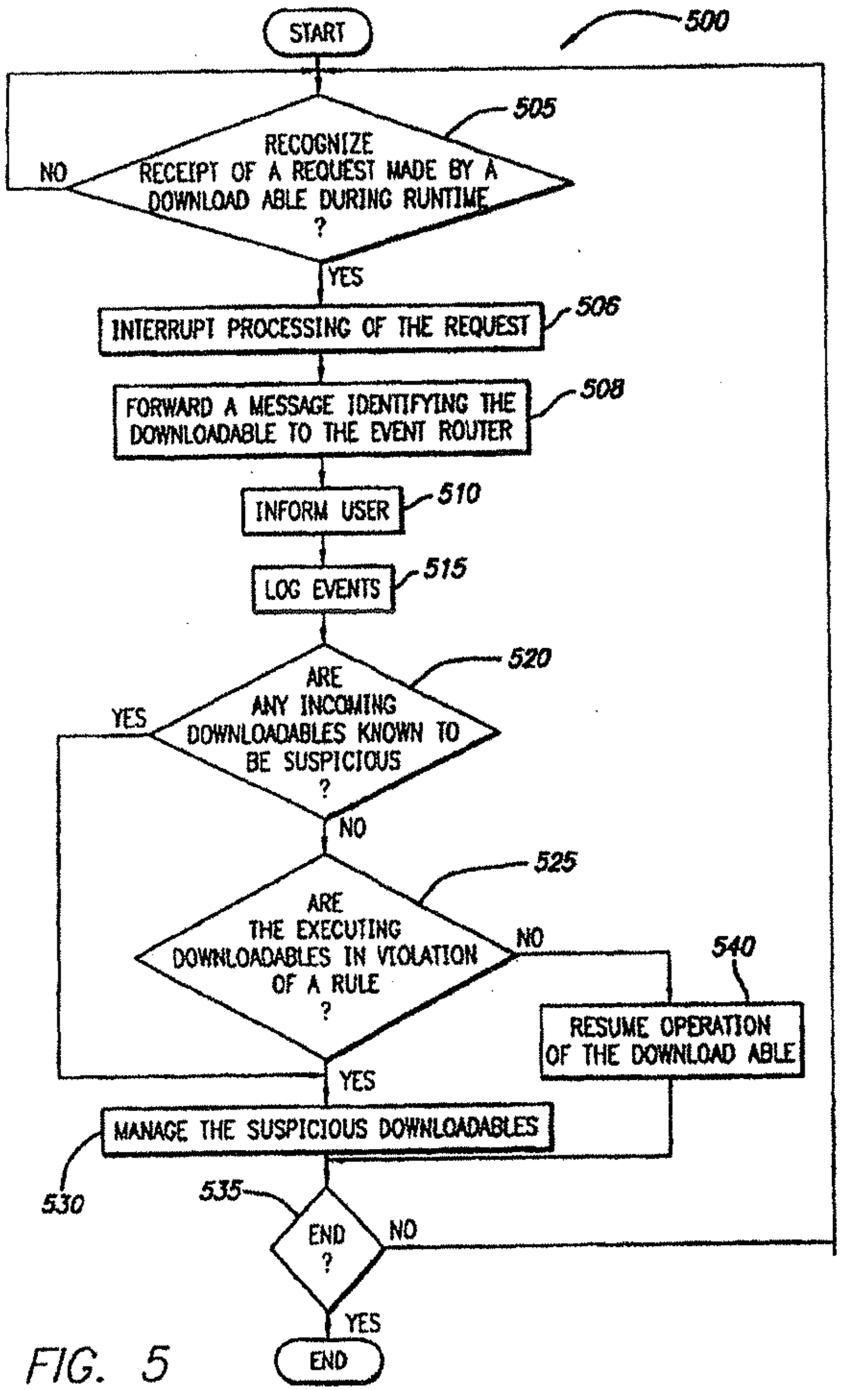

START
500
505
NO
RECOGNIZE RECEIPT OF A REQUEST MADE BY A DOWNLOAD ABLE DURING RUNTIME ?
YES
INTERRUPT PROCESSING OF THE REQUEST
506
FORWARD A MESSAGE IDENTIFYING THE DOWNLOADABLE TO THE EVENT ROUTER
508
INFORM USER
510
LOG EVENTS
515
520
YES
ARE ANY INCOMING DOWNLOADABLES KNOWN TO BE SUSPICIOUS ?
NO
525
ARE THE EXECUTING DOWNLOADABLES IN VIOLATION OF A RULE ?
NO
540
RESUME OPERATION OF THE DOWNLOAD ABLE
YES
MANAGE THE SUSPICIOUS DOWNLOADABLES
530
535
END ?
NO
YES
END

FIG. 5

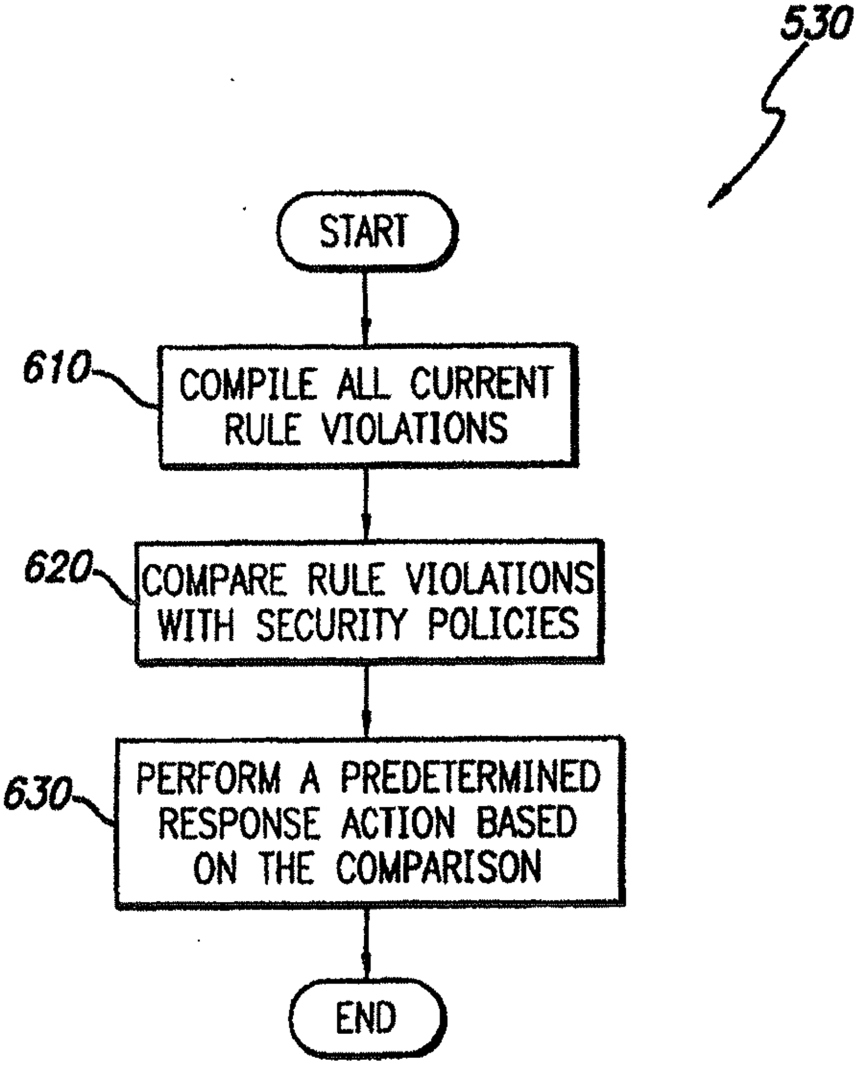

530
START
610
COMPILE ALL CURRENT RULE VIOLATIONS
620
COMPARE RULE VIOLATIONS WITH SECURITY POLICIES
630
PERFORM A PREDETERMINED RESPONSE ACTION BASED ON THE COMPARISON
END

FIG. 6

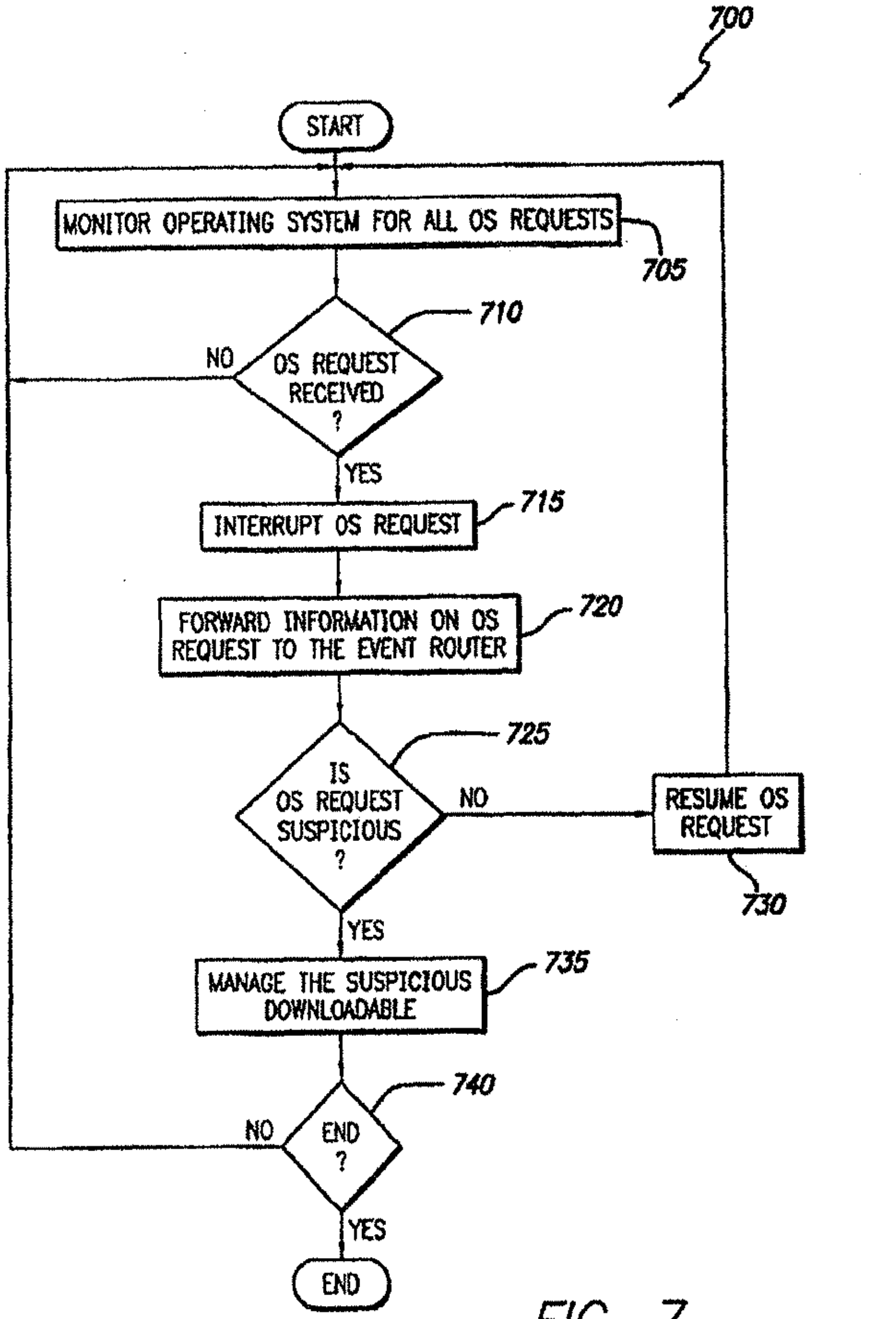

700
START
MONITOR OPERATING SYSTEM FOR ALL OS REQUESTS
705
710
OS REQUEST RECEIVED ?
NO
YES
INTERRUPT OS REQUEST
715
FORWARD INFORMATION ON OS REQUEST TO THE EVENT ROUTER
720
725
IS OS REQUEST SUSPICIOUS ?
NO
RESUME OS REQUEST
730
YES
MANAGE THE SUSPICIOUS DOWNLOADABLE
735
740
END ?
NO
YES
END

FIG. 7

SYSTEM AND METHOD FOR PROTECTING A CLIENT DURING RUNTIME FROM HOSTILE DOWNLOADABLES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to co-pending provisional patent application filed on Nov. 8, 1996, entitled "System and Method for Protecting a Computer from Hostile Downloadables," Ser. No. 60/030,639, by inventor Shlomo Touboul, which subject matter is hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for protecting clients from hostile Downloadables.

2. Description of the Background Art

The Internet currently interconnects about 100,000 individual computer networks and several million computers. Because it is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

In response to the widespread generation and distribution of computer viruses, programmers continue to design and update security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are typically not configured to recognize computer viruses which have been attached to or masked as harmless Downloadables (i.e., applets). A Downloadable is a small executable or interpretable application program which is downloaded from a source computer and run on a destination computer. A Downloadable is used in a distributed environment such as in the Java™ distributed environment produced by Sun Microsystems or in the ActiveX™ distributed environment produced by Microsoft Corporation.

Hackers have developed hostile Downloadables designed to penetrate security holes in Downloadable interpreters. In response, Sun Microsystems, Inc. has developed a method of restricting Downloadable access to resources (file system resources, operating system resources, etc.) on the destination computer, which effectively limits Downloadable functionality at the Java™ interpreter. Sun Microsystems, Inc. has also provided access control management for basing Downloadable-accessible resources on Downloadable type. However, the above approaches are difficult for the ordinary web surfer to manage, severely limit Java™ performance and functionality, and insufficiently protect the destination computer.

Other security system designers are currently considering digital signature registration stamp techniques, wherein, before a web browser will execute a Downloadable, the Downloadable must possess a digital signature registration stamp. Although a digital signature registration stamp will diminish the threat of Downloadables being intercepted, exchanged or corrupted, this approach only partially addresses the problem. This method does not stop a hostile Downloadable from being stamped with a digital signature, and a digital signature does not guarantee that a Downloadable is harmless. Therefore, a system and method are needed for protecting clients from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a client from hostile Downloadables. The system includes security rules defining suspicious actions such as WRITE operations to a system configuration file, overuse of system memory, overuse of system processor time, etc. and security policies defining the appropriate responsive actions to rule violations such as terminating the applet, limiting the memory or processor time available to the applet, etc. The system includes an interface, such as Java™ class extensions and operating system probes, for receiving incoming Downloadable and requests made by the Downloadable. The system still further includes a comparator coupled to the interface for examining the Downloadable, requests made by the Downloadable and runtime events to determine whether a security policy has been violated, and a response engine coupled to the comparator for performing the violation-based responsive action.

The present invention further provides a method for protecting a client from hostile Downloadables. The method includes the steps of recognizing a request made by a Downloadable during runtime, interrupting processing of the request, comparing information pertaining to the Downloadable against a predetermined security policy, recording all rule violations in a log, and performing a predetermined responsive action based on the comparison.

It will be appreciated that the system and method of the present invention use at least three hierarchical levels of security. A first level examines the incoming Downloadables against known suspicious Downloadables. A second level examines runtime events. A third level examines the Downloadables operating system requests against predetermined suspicious actions. Thus, the system and method of the invention are better able to locate hostile operations before client resources are damaged.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a network system in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of the client;

FIG. 3 is a block diagram illustrating details of a security system;

FIG. 4 is a block diagram illustrating details of an alternative security system;

FIG. 5 is a flowchart illustrating a method for protecting a client from suspicious Downloadables;

FIG. 6 is a flowchart illustrating the method for managing a suspicious Downloadable; and

FIG. 7 is a flowchart illustrating a supplementary method for protecting a client from suspicious Downloadables.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating a network system 100 in accordance with the present invention. Network system 100 includes a server 110 coupled to a communications channel 120, e.g., an Internet or an Intranet. The communications channel 120 is in turn coupled to a client 130, e.g., an individual computer, a network computer, a kiosk workstation, etc., which includes a security system 135 for protecting the client 130 from hostile (i.e., will adversely effect the operational characteristics of the client 130) or suspicious (i.e., potentially hostile) downloadables.

Server 110 forwards a Downloadable 140 across the communications channel 120 to the client 130. During runtime, the security system 135 examines each Downloadable 140 and the actions of each Downloadable 140 to monitor for hostile or suspicious actions.

FIG. 2 is a block diagram illustrating details of a client 130, which includes a Central Processing Unit (CPU) 205, such as a Motorola Power PC® microprocessor or an Intel Pentium® microprocessor, coupled to a signal bus 220. The client 130 further includes an input device 210 such as a keyboard and mouse, an output device 215 such as a Cathode Ray Tube (CRT) display, a data storage device 230 such as Read Only Memory (ROM) or magnetic disk, and a Random-Access Memory (RAM) 235, each being coupled to signal bus 220. A communications interface 225 is coupled between the communications channel 120 and the signal bus 220.

An operating system 260 controls processing by CPU 205, and is typically stored in data storage device 230 and loaded into RAM 235 for execution. The operating system 260 includes a file management system 265, a network management system 270, a process system 275 for controlling CPU 205, and a memory management system 280 for controlling memory use and allocation. A communications engine 240 generates and transfers message packets to and from the communications channel 140 via the communications interface 225, and may also be stored in data storage device 230 and loaded into RAM 235 for execution.

The client 130 further includes a web browser 245, such as the Netscape™ web browser produced by the Netscape Corporation, the Internet Explorer™ web browser produced by the Microsoft Corporation, or the Java™ Developers Kit 1.0 web browser produced by Sun Microsystems, Inc., for communicating via the communications channel 120. The web browser 245 includes a Downloadable engine 250 for managing and executing received Downloadables 140.

The client 130 further includes the security system 135 as described with reference to FIG. 1. The security system 135 may be stored in data storage device 230 and loaded into RAM 235 for execution. During runtime, the security system 135 intercepts and examines Downloadables 140 and the actions of Downloadables 140 to monitor for hostile or suspicious actions. If the security system 135 recognizes a suspicious Downloadable 140 or a suspicious request, then the security system 135 can perform an appropriate responsive action such as terminating execution of the Downloadable 140.

FIG. 3 is a block diagram illustrating details of the security system 135*a*, which is a first embodiment of security system 135 of FIG. 2 when operating in conjunction with a Java™ virtual machine 250 (i.e., the Downloadable engine 250) that includes conventional Java™ classes 302. Each of the Java™ classes 302 performs a particular service such as loading applets, managing the network, managing file access, etc. Although Downloadables are being described with reference to the Java™ distributed environment, Downloadables herein correspond to all downloadable executable or interpretable programs for use in any distributed environment such as in the ActiveX™ distributed environment.

Examples of Java™ classes used in Netscape Navigator™ include AppletSecurity.class, EmbeddedAppletFrame.class, AppletClassLoader.class, MozillaAppletContext.class, ServerSocket.class, SecurityException.class and SecurityManager.class, etc. Examples of Java™ classes used in Internet Explorer™ include AppletSecurity.class, BrowserAppletFrame.class, AppletClassLoader.class, ServerSocket.class, SecurityException.class and SecurityManager.class, etc. Other classes may include Broker.class, BCInterface.class, SocketConnection.class, queueManager.class, BrowserExtension.class, Message.class, MemoryMeter.class and AppletDescription.class.

The security system 135*a* includes Java™ class extensions 304, wherein each extension 304 manages a respective one of the Java™ classes 302. When a new applet requests the service of a Java class 302, the corresponding Java™ class extension 304 interrupts the request and generates a message to notify the request broker 306 of the Downloadable's request. The request broker 306 uses TCP/IP message passing protocol to forward the message to the event router 308.

The security system 135*a* further includes operating system probes 310, 312, 314 and 316. More particularly, a file management system probe 310 recognizes applet instructions sent to the file system 265 of operating system 260, a network system probe 312 recognizes applet instructions sent to the network management system 270 of operating system 260, a process system probe 314 recognizes applet instructions sent to the process system 275 of operating system 260, and a memory management system probe 316 recognizes applet instructions sent to the memory system 280 of operating system 260. When any of the probes 310–316 recognizes an applet instruction, the recognizing probe 310–316 sends a message to inform the event router 308.

Upon receipt of a message, the event router 308 accordingly forwards the message to a Graphical User Interface (GUI) 324 for notifying the user of the request, to an event log 322 for recording the message for subsequent analysis, and to a runtime environment monitor 320 for determining whether the request violates a security rule 330 stored in a security database 326. Security rules 330 include a list of computer operations which are deemed suspicious. Suspicious operations may include READ/WRITE operations to a system configuration file, READ/WRITE operations to a document containing trade secrets, overuse of system memory, overuse of system processor time, too many applets running concurrently, or too many images being displayed concurrently. For example, the runtime environment monitor 320 may determine that a security rule 330 has been violated when it determines that an applet uses more than two megabytes of RAM 235 or when the Java™ virtual machine 250 runs more than five applets concurrently.

Upon recognition of a security rule 330 violation, the runtime environment monitor 320 records the violation with the event log 322, informs the user of the violation via the GUI 324 and forwards a message to inform the response engine 318 of the violation. The response engine 318 analyzes security policies 332 stored in the security database 326 to determine the appropriate responsive action to the rule 330 violation. Appropriate responsive actions may include terminating the applet, limiting the memory or processor time available to the applet, etc. For example, the response engine 318 may determine that a security policy 332 dictates that when more than five applets are executed concurrently, operation of the applet using the greatest amount of RAM 235 should be terminated. Further, a security policy 332 may dictate that when an applet or a combination of applets violates a security policy 332, the response engine 318 must add information pertaining to the applet or applets to the suspicious Downloadables database 328. Thus, when the applet or applets are encountered again, the response engine 318 can stop them earlier.

The GUI 324 enables a user to add or modify the rules 330 of the security database 326, the policies 332 of the security database 326 and the suspicious applets of the suspicious Downloadables database 328. For example, a user can use the GUI 324 to add to the suspicious Downloadables database 328 applets generally known to be hostile, applets deemed to be hostile by the other clients 130 (not shown), applets deemed to be hostile by network MIS managers, etc. Further, a user can use the GUI 324 to add to the rules 330 actions generally known to be hostile, actions deemed to be hostile by network MIS managers, etc.

It will be appreciated that the embodiment illustrated in FIG. 3 includes three levels of security. The first level examines the incoming Downloadables 140 against known suspicious Downloadables. The second level examines the Downloadables' access to the Java™ classes 302. The third level examines the Downloadables requests to the operating system 260. Thus, the security system 135*a* is better apt to locate a hostile operation before an operation damages client 130 resources.

FIG. 4 is a block diagram illustrating details of a security system 135*b*, which is a second embodiment of security system 135 when operating in conjunction with the ActiveX™ platform (i.e., the Downloadable engine 250) which uses message 401 calls, Dynamic-Data-Exchange (DDE) 402 calls and Dynamically-Linked-Library (DLL) 403 calls. Thus, instead of having Java™ class extensions 304, the security system 135 has a messages extension 401 for recognizing message 401 calls, a DDE extension 405 for recognizing DDE 402 calls and a DLL extension 406 for recognizing DLL calls. Upon recognition of a call, each of the messages extension 404, the DDE extension 405 and the DLL extension 406 send a message to inform the request broker 306. The request broker 306 and the remaining elements operate similarly to the elements described with reference to FIG. 3.

FIG. 5 is a flowchart illustrating a method 500 for protecting a client 130 from hostile and suspicious Downloadables 140. Method 500 begins with the extensions 304, 404, 405 or 406 in step 505 waiting to recognize the receipt of a request made by a Downloadable 140. Upon recognition of a request, the recognizing extension 304, 404, 405 or 406 in step 506 interrupts processing of the request and in step 508 generates and forwards a message identifying the incoming Downloadable 140 to the request broker 306, which forwards the message to the event router 308.

The event router 308 in step 510 forwards the message to the GUI 324 for informing the user and in step 515 to the event log 322 for recording the event. Further, the event router 308 in step 520 determines whether any of the incoming Downloadables 140 either alone or in combination are known or previously determined to be suspicious. If so, then method 500 jumps to step 530. Otherwise, the runtime environment monitor 320 and the response engine 318 in step 525 determine whether any of the executing Downloadables 140 either alone or in combination violate a security rule 330 stored in the security database 332.

If a rule 330 has been violated, then the response engine 318 in step 530 manages the suspicious Downloadable 140. Step 530 is described in greater detail with reference to FIG. 6. Otherwise, if a policy has not been violated, then response engine 318 in step 540 resumes operation of the Downloadable 140. In step 535, a determination is made whether to end method 500. For example, if the user disconnects the client 130 from the server 110, method 500 ends. If a request to end is made, then method 500 ends. Otherwise, method 500 returns to step 505.

FIG. 6 is a flowchart illustrating details of step 530. Since multiple rule 330 violations may amount to a more serious violation and thus require a stricter response by the response engine 318, step 530 begins with the response engine 318 in step 610 compiling all rule 330 violations currently occurring. The response engine 318 in step 620 compares the compiled rule 330 violations with the security policies 332 to determine the appropriate responsive action for managing the suspicious Downloadable 140 or Downloadables 140, and in step 630 the response engine 318 performs a predetermined responsive action. Predetermined responsive actions may include sending a message via the GUI 324 to inform the user, recording the message in the event log 322, stopping execution of a suspicious Downloadable 140, storing a Downloadable 140 or combination of Downloadables 140 in the suspicious Downloadable database 328, limiting memory available to the Downloadable 140, limiting processor time available to the Downloadable 140, etc.

FIG. 7 is a flowchart illustrating a supplementary method 700 for protecting a client 130 from suspicious Downloadables 140. Method 700 begins with operating system probes 310, 312, 314 and 316 in step 705 monitoring the operating system 260 for Operating System (OS) requests from Downloadables 140. As illustrated by step 710, when one of the probes 310–316 recognizes receipt of an OS request, the recognizing probe 310–316 in step 715 interrupts the request and in step 720 forwards a message to inform the event router 308.

The event router 308 in step 725 routes the information to each of the components of the security engine 135 as described with reference to FIG. 5. That is, the event router 308 forwards the information to the GUI 324 for informing the user, to the event log 322 for recordation and to the runtime environment monitor 320 for determining if the OS request violates a rule 330. The response engine 318 compares the OS request alone or in combination with other violations against security policies 332 to determine the appropriate responsive actions. It will be appreciated that, based on the security policies 332, the response engine 318 may determine that an OS request violation in combination with other OS request violations, in combination with rule 330 violations, or in combination with both other OS request violations and rule 330 violations merits a stricter responsive action.

If the OS request does not violate a security rule 330, then the response engine 318 in step 730 instructs the operating system 260 via the recognizing probe 310–316 to resume operation of the OS request. Otherwise, if the OS request violates a security rule 330, then the response engine 318 in step 730 manages the suspicious Downloadable by performing the appropriate predetermined responsive actions as described with reference to FIGS. 5 and 6. In step 740, a determination is made whether to end method 700. If a request to end the method is made, then method 700 ends. Otherwise, method 700 returns to step 705.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method, comprising:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

2. A computer-based method, comprising:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

3. A system, comprising:

a security policy;

an operating system interface for recognizing a runtime event caused from a request made by a Downloadable;

a comparator coupled to the interface for comparing information pertaining to the received Downloadable with the security policy;

a response engine coupled to the comparator for performing a predetermined responsive action based on the comparison with the security policy; and

an event log coupled to the comparator for storing results of the comparison.

4. A system, comprising:

a security policy;

an operating system interface for recognizing a runtime event caused from a request made by a Downloadable;

a comparator coupled to the interface for comparing information pertaining to the received Downloadable with the security policy;

a response engine coupled to the comparator for performing a predetermined responsive action based on the comparison with the security policy; and

a suspicious Downloadable database for storing known and previously-deemed suspicious Downloadables.

5. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

6. A system for determining whether a Downloadable, which is received by a Downloadable engine, is suspicious, comprising:

means for monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

means for interrupting processing of the request;

means for comparing information pertaining to the Downloadable against a predetermined security policy; and

means for performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

7. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing results of the comparison in an event log.

8. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

monitoring the operating system during runtime for an event caused from a request made by a Downloadable;

interrupting processing of the request;

comparing information pertaining to the Downloadable against a predetermined security policy; and

performing a predetermined responsive action based on the comparison, the predetermined responsive action including storing the Downloadable in a suspicious Downloadable database.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,167,520
DATED : December 26, 2000
INVENTOR(S) : Shlomo Touboul

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page,
Item [73], Assignee, "Finjan Software, Inc., San Jose, Calif.," after "Finjan Software," change "Inc., San Jose, Calif." to -- Ltd., Kefar Haim, Israel --.

Signed and Sealed this

Seventh Day of February, 2006

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office

Exhibit 4

EXHIBIT
JARR-19
RJ 12-17-07
PENGAD 800-631-6989

Cooley
GODWARD KRONISH LLP

Wayne O. Stacy
(720) 566-4125
wstacy@cooley.com

March 26, 2007

VIA FAX 650-838-4350

Paul J. Andre, Esq.
Perkins Cole
101 Jefferson Drive
Menlo Park, CA 94025-1114

RE: U.S. PATENT NOS. 6,167,520 AND 6,480,962

Dear Paul:

We represent Webroot Software, Inc. ("Webroot"), and we write in response to your March 5, 2007 letter.

We welcome the opportunity to meet with you in Colorado to discuss the '520 and '960 patents. Prior to any meeting, however, we must better understand your positions. To that end, we ask that you identify the claims and the corresponding features of Webroot's Spy Sweeper product that you would like to discuss. Additionally, we ask that you provide us with constructions for the following claim terms: "Downloadable;" "predetermined security policy;" "monitoring the operating system;" and "response engine." To the extent you would like to discuss any mean-plus-function claims, please identify the corresponding structure in the specification.

Once we have received and reviewed this information we will call you to schedule the meeting.

Regards,

COOLEY GODWARD KRONISH LLP

Stacy

Wayne O. Stacy

271998 v1/CO

Defendant's Trial Ex.
DTX - 1306
Case No. 06-369 GMS

Exhibit 5

Conference Call Transcript

SCUR - Q1 2008 Secure Computing Corporation Earnings Conference Call

Event Date/Time: May. 01. 2008 / 4:30PM ET

CORPORATE PARTICIPANTS

Jane Underwood
Secure Computing Corporation - IR

Tim Steinkopf
Secure Computing Corporation - SVP of Operations & CFO

Dan Ryan
Secure Computing Corporation - CEO

CONFERENCE CALL PARTICIPANTS

Eric Martinuzzi
Craig-Hallum Capital Group - Analyst

Rob Owens
Pacific Crest Securities - Analyst

Jonathan Ruykhaver
ThinkEquity Partners - Analyst

Fred Ziegel
Soleil Securities - Analyst

Josh Jabs
Roth Capital Partners - Analyst

Fred Green
Goldman Sachs - Analyst

Joe Maxa
Dougherty & Company - Analyst

Katherine Egbert
Jefferies & Company - Analyst

Eric Suppiger
Signal Hill Group LLC - Analyst

Todd Raker
Deutsche Bank - Analyst

Joel Fishbein
Lazard Capital Markets - Analyst

PRESENTATION

Operator

Welcome to Secure Computing Corporation's first quarter 2008 results conference call. All participants will be able to listen only until the question and answer session, which will follow today's presentation. (OPERATOR INSTRUCTIONS) Today's call is being recorded. If there are any objections, please disconnect at this time. I will now turn the call over to Miss Jane Underwood, Vice President for Investor Relations.

Jane Underwood - ***Secure Computing Corporation - IR***

Good afternoon. And thanks for joining us to discuss our first quarter results. On the call with me today with Dan Ryan, our CEO; and Tim Steinkopf, our Senior Vice President of Operations and CFO.

Before I turn the call to Tim, I'm going to make a cautionary statement regarding forward-looking statements. During the course of this call and the question and answer session following management's remarks, we will make forward-looking statements that involve risks and uncertainties.

Such forward-looking statements are subject to the Safe Harbor created by the Private Securities Litigation Reform Act of 1995. These statements include, for example, statements regarding future results such as guidance for second quarter billings, revenue, gross margin, operating expense, tax expense, interest and other expense, expense reductions, shares outstanding, earnings per share and cash flows and cash balances and statements about our sales pipeline, the breakdown of sales across our product lines and success and availability of our products. Our actual results could differ materially from the forward-looking statements. Factors which could cause actual results to differ include for example risks related to the competition in the securities industry, changes in customer requirements, delays in product development, and the other factors and risks identified in our press release and our SEC filings. We do not undertake any obligation to correct or update any forward-looking statements that may become inaccurate. Now, I would like the turn the call over to Tim.

Tim Steinkopf - ***Secure Computing Corporation - SVP of Operations & CFO***

Thank you, Jane. Since our final Q1 results are consistent with the preliminary results that we announced on April 7th, we'll briefly review the highlights for the quarter and then spend some time discussing a few cost-saving measures that we undertook this past week. As a reminder, non-GAAP financial measures are reconciled to GAAP in the table at the end of today's press release. Non-GAAP revenue for the first quarter was $65.7 million, an 8% increase over the prior year. Billings for the first quarter were $69.1 million, a 4% increase over a year. Non-GAAP net income for Q1 was $5 million or $0.07 per fully diluted share.

The shortfall relative to our guidance issued on February 4th was largely related to the two issues that we discussed on April 7th. First, our North America commercial business was significantly impacted by a combination of macroeconomic headwinds causing customers to delay purchasing decisions. Second, our U.S. Federal team fell short of their goal due to contracting delays and budgeting issues related to the continuing resolution that the government was operating under at that time. In the last six business days of the quarter, approximately $11 million of revenue from our commit line was pushed out of Q1. Importantly, our EMEA and Asia Pac teams experienced very solid performance, delivering at or close to their target.

In Q1, international billings were 41% of total billings. Domestic billings, excluding the U.S. federal government were 42% of total billing, and the U.S. federal government represented 17% of our total billing. In the first quarter, billings for our gateway security products were 86% of total billing and billings for identity and access products were 14% of total billing. In the quarter, we closed five individual transactions greater than $1 million and an additional 110 deals over $100,000. Deferred revenue increased $6.2 million or 4% sequentially. At end of March, the total deferred revenue balance was $174.4 million. As expected, non-GAAP gross margin was 75% of revenue. Non-GAAP operating income for the quarter was 10% of revenue. In Q1, we generated a $13.1 million in cash from operations. The company's cash and restricted cash balance was $23.7 million on March 31st.

Before I turn to Q2 guidance, I would like to discuss the cost-saving measures we undertook this past week. These measures included the elimination of 75 open positions that we had been planning to fill, the elimination of 75 current positions, additional reductions in non employee-related expenses from plan levels by $500,000 per quarter, and additionally we've reduced our planned capital spending by approximately $5 million for the balance of the year. A few other items to stress. We are maintaining an appropriate headcount in investment and engineering in order to continue fostering innovation, and the steps taken should reduce our forecasted expenses for 2008 by approximately $10 million, which equates to an annual amount of approximately $14 million to $15 million.

Now I would like to turn to our outlook guidance, which is based on current expectations. All of these statements are forward looking and actual results could differ materially. For the second quarter 2008, we expect billings to be up slightly from Q1. Non-GAAP revenue is expected to be in the range of $63 million to $67 million. Non-GAAP gross margin is anticipated to be approximately 73 to 75% of non-GAAP revenue. Non-GAAP operating expenses are expected to be in the range of $42 million to $43 million. Fully diluted weighted average share count is expected to be approximately 75 million shares. Non-GAAP tax expense, which is also approximate, our actual cash outlay for taxes is expected to be approximately $300,000 to $500,000.

Interest and other expense are expected to be approximately $900,000, and Q2 non-GAAP earnings per share is expected to be approximately $0.04 to $0.07 per fully diluted share. We again expect the breakdown of our product lines in Q2 to be approximately 90% for enterprise gateway and approximately 10% for identity and access management. As in prior years, we expect to see a sequential decrease in our Q2 cash generation due to normal seasonality. In Q2, cash generated from operations is expected to be approximately $3 million to $4 million. And consistent with normal seasonality, we would expect Q3 cash generation from operation to increase to approximately $6 million to $8 million. We expect Federal billings for Q2 to account for 15 to 20% of total billings.

And before I turn the call over to Dan, I would like to point out that we're suspending full year '08 and '09 guidance. Given the uncertain macroeconomic guidance and the amount of deal slippage we experienced in Q1, we believe it's prudent to only provide Q1 guidance at this time. I'd like to turn the call over to Dan.

Dan Ryan - *Secure Computing Corporation - CEO*

Thank you, Tim, and good afternoon. We are disappointed with our Q1 results and are taking aggressive actions to improve our future performance. This includes restructuring described by Tim and the implementation of a growth plan that I will briefly describe now. Over the last several months, the senior management team has been developing a strategy that will allow us to better capitalize on the market opportunities before us and provide stronger top and bottom line growth. Our board of directors has endorsed this plan and we're now aggressively executing on it.

While there's certainly excellent growth opportunities for each of our product lines, I'm a big believer in focus. Our increased focus will take two forms. First, we will commit substantially more of our resources to the areas of our business where we believe we can be the clear market leader. And second, we'll narrow the scope on our remaining products to the market segments where we have proven success and an opportunity for segment leadership. Regarding the former, our simple objective is to become the clear leader in secure web gateway market over the next 18 months and to remain a leader in the e-mail gateway market. The secure web gateway is a lucrative golden opportunity, and we are already in the strong position there. According to Gardner, there's only a 10 to 15% penetration of these solutions in the enterprise and 20 to 25% annual growth is anticipated.

Hosted web security, while smaller today than appliance base, is expected to grow at 36% annually according to IDC. We plan to address the web gateway market with flexible hybrid delivery model and that means appliance based virtualized and hosted or in the cloud offerings. In the coming weeks, we will launch a hosted web security service to complement our already successful appliance based offerings as well as our recently announced virtual offerings.

The new SAS, or software to service offering, leverages our web gateway technology as well as the worldwide data center infrastructure that exists for TrustedSource today. We're excited about both our current situation, as this is our most successful growth area, and the ability to accelerate this area based on an incremental investment combined with the high growth opportunity in the market. We remain a leader in the secure mail gateway market as well, which is another attractive growth area and one that has substantial synergies with web security. Similarly, we plan to offer flexible delivery models to our customers there.

In summary, our long-term strategy for web and mill security is to allow our customers to purchase market-leading security services and deploy them across different platforms to mix and match any configuration. This will deliver service portability, common policy in reporting, and unified pricing across all delivery models. Next, with respect to narrowing our scope on the remaining products, we have an excellent franchise in secure firewall or Sidewinder, the industry's leading application firewall. Our success in government financial services and high assurance networks in regulated and other industries continues to be strong. We protect some of the world's most critical networks and applications. If there's valuable data to be protected, we are a strong solution that should be considered.

Secure's firewall is also unique in that it's a software product that is readily virtualized and we will take advantage of that as well. Also, we offer the only application firewall that's fully integrated with the Reputation system, our TrustedSource system. Our emphasis going forward will be to aggressively attack and lead these key segments of the broader firewall market. Similarly, with SafeWord, we have a great platform to build from with the reformulated users today. Our primary emphasis will continue to be remote access solutions that can be rapidly deployed in Microsoft centric environments.

To summarize, we've reduced our cost structure and we are substantially increasing our investment in the high-growth areas where we believe we have the opportunity for clear leadership. In the other areas, we're narrowing our scope, and we will continue to strengthen our team throughout the organization. To that end, I'm pleased to announce that Steve Kozachok will be joining Secure Computing next week as our new Senior Vice President, Secretary, and General Counsel. Steve comes to us from St. Jude Medical, where he served as Associate General Counselor for the last three years and was the primary lawyer responsible for business development efforts. Before that, Steve was a partner in the law firm of Dorsey & Whitney, where he was Lead Outside Merger and Acquisition Counsel to a Fortune 50 company. I speak for the entire management team in saying we remain highly optimistic about the future of Secure. Operator, we would now like to open the call to analysts' questions.

QUESTION AND ANSWER

Operator

(OPERATOR INSTRUCTIONS) Our first question comes from Joel Fishbein with Lazard. Your line is open.

Joel Fishbein *- Lazard Capital Markets - Analyst*

A couple of questions. First can you give us more color on some of the product lines, Webwasher and Ironmail in particular, your secure web or secure mail, how they did in the quarter?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

We don't typically segment them out, but I will say that the -- our web gateway product line is certainly the highest growth area and is growing significantly higher than those market rate growths that we mentioned from Gardner's perspective, but beyond that we don't segment them.

Joel Fishbein *- Lazard Capital Markets - Analyst*

How about in terms of the competitive landscape there? Any better, any worse?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

I think that we're seeing the same competitors on the web gateway. I think that we feel we have an opening door to walk through or jump through, run through or whatever you say, that some of our competitors are quite busy with either digesting acquisitions or just embarking on them, a couple of our primary competitors. We're hoping that gives us a little bit more of an entry to really take that market. Our intention here is to dominate the web gateway market and that's really what you're going to see focus of this company be for the next year.

Joel Fishbein *- Lazard Capital Markets - Analyst*

The second question comes, regarding, Tim, you talked about last quarter. On the last call, about $11 million got pushed from Q1. And even assuming you got half of that in Q1, you would have crushed the number. Why the lower guidance for Q2?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

Yes, we've never had that many deals or that amount of deals slip out of the end of a quarter as we discussed on the 7th. And although there are some results out there that did fine for Q1 and said they were fine for North America, there were certainly other data points where there is concerns about the North America economy, market, macroeconomic environment, et cetera. Given that we're looking at a phenomenon at the end of Q1 that we've never seen before and the overall macro environment in the Americas especially, we felt it to be prudent to be conservative as look into Q2.

Joel Fishbein *- Lazard Capital Markets - Analyst*

All right. I'll jump back into queue. Thanks.

Operator

Eric Martinuzzi, your line is open with Craig Hallum.

Eric Martinuzzi *- Craig-Hallum Capital Group - Analyst*

Curious, given the guidance on the billings for Q2, I think up slightly from Q1 is the way you characterized it. That would imply a decline from a year ago. A year ago we had -- I think billings were $70.7 million or so. So up slightly. Is that $69.5 million or is that $71 million? Could we be in a contracting mode here for the foreseeable future?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

I think we would say that we expect to be may be up slightly from prior year as well. But, again, when you look at the macro environment, we feel it prudent to look hard at the pipeline we have and feel comfortable with what's in that pipeline relative to expectations to close and guide appropriately. And that still means that there's basically two months to go on this quarter. There's a lot of work to get done.

Eric Martinuzzi *- Craig-Hallum Capital Group - Analyst*

One more if I might. One of the things you've done is looked at your cost structure. What about your business segments? Is that on the table? Could we see potential strategic diversification here where maybe we aren't in certain businesses in the future that we currently are in?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

I don't think we have any particular plans to announce there, but I would say in looking at our strategy, anything's on the table. We'll do anything that we think maximizes the shareholder value and our growth opportunity and whether that's acquisitions or doing what you suggested.

Eric Martinuzzi *- Craig-Hallum Capital Group - Analyst*

Thank you.

Operator

Rob Owens with Pacific Crest Securities, your line is open.

Rob Owens *- Pacific Crest Securities - Analyst*

Yes, good afternoon, everyone.

Dan Ryan *- Secure Computing Corporation - CEO*

Hi, Rob.

Rob Owens *- Pacific Crest Securities - Analyst*

Any type of update you can give us with regard to the lawsuit with Finjan, where you're at in that process?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

Where the status is -- the jury has entered a verdict against us. We won on one count on the trial. They won on two counts. There was a verdict entered against us, and we have filed motions relative to that, we were asking the judge to set that aside, reduce the damages, et cetera, et cetera. Of course, Finjan has also filed motion for an injunction. All of the typical motions that both sides would file. We expect the judge to rule on those motions in three to five months, so sometime maybe in Q2. It might slip into July/August. Can't readily predict that. I'm sure whoever comes out on the short end of the judge's ruling will file appeals to the appellate court and that will take one year to two years to play out. A lot of game to be played there yet. As we've stated before, we don't believe that's going to be a material item to the company when it eventually does get resolved. But it's probably at least 1.5 years plus time rame before it's finally all put to rest.

Rob Owens *- Pacific Crest Securities - Analyst*

Along those lines, is that causing any disruption in the selling process? Customer adoption team, I guess?

Dan Ryan *- Secure Computing Corporation - CEO*

It's certainly been distracting to us as a company. I think obviously Finjan is putting this out in the market in front of a lot of prospective customers and trying to make something of that. I would say that -- I am aware of one substantial deal that we would directly relate to this. We're not aware of any other ones at this time. They may exist, but we're not aware of them, and there was one specific one we know. We should also -- I'm sure you've heard this before this infringement isn't about the broader Webwasher product line. It's about one element of that product line and we do have the ability to ship the product today without the alleged infringement if we chose to do that. We are obviously not choosing to do that, and we have a long ways to go in the fight. So I think -- another thing is we don't really see Finjan competing with us in many deals. The [Fillmore], the Bluecoats and WebCensus we're seeing on the Webwasher side. But I would say it hasn't been a terrible business environment for us because of it. It has been some distraction to it and there is some small business impact.

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

It's kind of a nuisance on the side. It's there. We have to deal with it. We don't see them that much, but it is a bit nuisance. You couldn't say it's had zero impact. It's been a nuisance.

Rob Owens *- Pacific Crest Securities - Analyst*

Great, thanks.

Operator

Jonathan Ruykhaver with ThinkEquity, your line is open.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

Good afternoon. It looks like you incurred $2 million in legal expenses related to Finjan. Is that the type of run rate we should expect in terms of cash expense in the next few quarters?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

No. So, yes, you're correct we did incur a fairly significant item in Q1 because of the trial, et cetera. But going forward, probably $300,000 to $400,000 a quarter for a couple quarters or two or three quarters has been built in. That's what we would expect to incur for the balance of the year.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

That's not included in the non-GAAP guidance you gave?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

It is included.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

It is. Okay.

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

It is included.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

In terms of the $11 million deals that slipped out of March, would you characterize most of those as network security products?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

We looked at that and yes, probably more gateway security then I am, but in some respects fairly evenly spread out across all four product lines.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

So you even saw some pushed out of the web security side?

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

Yes, and it wasn't necessary to any product line. It seemed to be more focused by geography because we didn't see the slippage in EMEA in any type of product line nor in Asia Pac, but we saw it in North America and a little bit in lap and North America especially, and it seemed to be across all product lines. But at the end of the day, as Dan stated in either one of his questions or prepared remarks, was we still are seeing as far as all of the product lines go, an IDC would probably back this up as well. Our best growth opportunity, and we're seeing it in our activity, is in the web gateway area.

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

Right. And I guess just going back to the network gateway marketplace. Is there a contraction that's occurring in that marketplace or is there heightened competition? I'm trying to get a sense of what is causing the problems in that particular market, because I think most of your gateway business is probably in the firewall marketplace.

Dan Ryan *- Secure Computing Corporation - CEO*

I don't think -- we have three gateway products: mail, web and firewall. I would say, as Tim said, there's some contraction in each. I don't think we're seeing any particular fallback in our network gateway business. We actually had a nice growth in that business over the past year. I think that the -- it doesn't have the kind of growth we're seeing in web gateway, but I don't think we've seen a particular fallback. We focus in on we have a very good position, I don't know if you call it a niche market or a sub segment of these high assurance network and we do a lot in government and financial services. And there's a lot of initiatives that are supporting whatever downturn there is economically when you have [PCI DFF] initiatives and this critical infrastructure initiatives are going on right now. We're in a lot of those deals. I wouldn't say that there was a pretty good fallout in our network gateway any more than any other --

---

Jonathan Ruykhaver *- ThinkEquity Partners - Analyst*

Year-over-year looking at the billings growth being flat year-over-year for the most part and you're saying the web gateway business is growing and mail is probably doing okay. It would have to be either the authentication or the firewall business that's been showing accelerated growth.

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

Maybe another way to think about it is when the markets -- we perceive the markets to still be strong, it's just that they seem to be a little bit pressured right now. But we don't perceive it to be in the market. We perceive it more in the macroeconomic environment. Products are not going away -- they're getting pushed out. People are not saying they're not important or they're not going to do it. They're saying I need to get another signature or need to go back through CapEx committee or it's going to take us longer to get approved. What we're seeing is more of a macro pressure from the environment than a specific segment of the market that's kind of backing up.

Jonathan Ruykhaver - *ThinkEquity Partners - Analyst*

Okay. So is it safe to assume that based the revenue guidance for June, you're being pretty conservative still as it relates to closure rates, sales cycles, continue to deteriorate?

Dan Ryan - *Secure Computing Corporation - CEO*

That would be the way to think about it.

Jonathan Ruykhaver - *ThinkEquity Partners - Analyst*

All right, guys. Thanks.

Operator

Fred Ziegel with Soleil Securities, your line is open.

Dan Ryan - *Secure Computing Corporation - CEO*

Hey, Fred.

Fred Ziegel - *Soleil Securities - Analyst*

Let me ask a couple of things. First, on the bigger deals, I would presume they are generally multi-product in terms of people looking at doing a couple of different things?

Dan Ryan - *Secure Computing Corporation - CEO*

Probably more often they're not, actually, Fred. I would say many of the big deals tend to be single product, kind of enterprise rollout or enterprise deployment. We do have multi-product deals all the time, but I wouldn't characterize -- if you went through our biggest deals, they're more likely to be one product than they are to be three.

Fred Ziegel - *Soleil Securities - Analyst*

Okay.

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

I agree and what that actually provides us is the opportunity to cross sell which we're definitely seeing an uptick in.

Fred Ziegel - *Soleil Securities - Analyst*

But if we're going to defocus some areas of the business, does that opportunity go away?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

No, because I think what maybe -- paraphrase Dan's comments, it is focus in on the areas where each product is the strongest. So web and mail happen to be strong in broad areas and we can look to be market leaders there in broad areas. Whereas secure firewall, secure IM, they are potentially a little bit more focused or have the opportunity to be leaders in a little bit more focused area. And that's where we will have the most success cross selling also. It's focusing in where we're the strongest.

Dan Ryan - *Secure Computing Corporation - CEO*

If we have an account that's a big Webwasher account and they're looking for firewalls, we're not going to tell the salesperson not to introduce Sidewinder to the account because it's not in one of the key verticals. In reality, we'll have more cross selling in the two or three verticals for firewall than we would in the general world.

Fred Ziegel - *Soleil Securities - Analyst*

The 75 person headcount reduction -- how is that spread out across the various disciplines?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

We tried very hard to impact sales generation the least amount as possible, and we tried also to impact our development team probably second least amount possible. So what I'll call the service organizations within the company, legal, HR, marketing -- we tried also to limit the impact to marketing. That probably was third in line. But then the service organizations, the balance of marketing, legal, HR, finance, operations, IT, et cetera -- those groups really stepped up and said we're going to try to cut our costs as aggressively as possible because we want to maintain our investment in innovation and the road maps we're on and want to maintain the lead generation pipeline generation machine.

Dan Ryan - *Secure Computing Corporation - CEO*

Hopefully it's clear also from the discussion that we not only took that money out of the company that Tim described. We added specifically a substantial amount of money back to the web gateway development and go to market areas. So that's all built into the numbers that we gave you. So the actual cut was probably more substantial when you consider that addback.

Fred Ziegel - *Soleil Securities - Analyst*

Okay. All right, thanks.

Operator

Josh Jabs with Roth Capital, your line is open.

Josh Jabs - *Roth Capital Partners - Analyst*

Good afternoon.

Dan Ryan - *Secure Computing Corporation - CEO*

Hey, Josh.

Josh Jabs - *Roth Capital Partners - Analyst*

On the previous call, you talked about the government sector, the Federal sector, and some of the issues that you had seen in Q1. How is that looking for Q2 and Q3?

Dan Ryan - *Secure Computing Corporation - CEO*

I would say we're cautiously optimistic about the U.S. federal government plan right now. Obviously we're fool me once or fool me once, right? But we're being cautious and I think we're seeing a strong opportunity there, a good comeback.

Josh Jabs - *Roth Capital Partners - Analyst*

And then, going back to this product diversification or consolidation or however this plays out. You mentioned the area of focus. At the same time, it seems like the market has been looking for more consolidated offerings. Specifically, how do you pull back in one area such as UTM, but continue to invest the others and does that mean more of a downmarket shift with the service's offerings?

Dan Ryan - *Secure Computing Corporation - CEO*

I think when you talk about the combination, the natural synergy is between web and mail. There's a much more natural synergy in selling those products together. And that is a consolidated offering. If you look at what we're doing, we're trying to come up with a set of services, web and mail-based services, that we don't care which ones you pick and how you want it delivered, whether it's in a box in the cloud. That is very synergistic, more so than with the firewall, with the firewall business I think. I would we're not trying to necessarily narrow our product breadth. However, we do want to be known for something and secure computing in the broader sense really hasn't been known for something. And our objective here is we want to take leadership in a market. That'll accelerate our channel and accelerate our customer acquisition. And then we can bring all of our other products into it as well.

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

I would submit to you, Josh, I think we're potentially a step or two or three ahead of our competitors in consolidation. We already consolidate at the web gateway services such as FSL, SML or anti-virus, web filtering, et cetera. We have the same type of consolidated services at the mail gateway with DLP encryption, AV, TrustedSource reputation. We have trusted reputation-based technology at the web as well. And look at our set of services at the enterprise gateway. I think Secure has actually been a leader in consolidating services at appropriate areas or appropriate spots in the network. Now what we're saying is we're going to take those spots and really focus in on trying to capitalize on our leadership there.

Dan Ryan - *Secure Computing Corporation - CEO*

One more example -- Tim brought up some good ones -- that the mail and web gateway, there's a lot of discussions in the market today about daily prevention or protection DLP. A lot of companies that we partner with on a regular basis in our web gateway solution. With these services, we have between web and mail, the vast majority of the deal [promised] in motion between those protocols, web and mail. One of the thing we want to do is provide DLP services with policy across them. We're going to continue consolidate, for in motion date. We're not trying to replace Vontu anybody on desktop-type applications, but the 80/20 rule is if you can stop the majority of it there, that's another great service we can consolidate.

Josh Jabs - *Roth Capital Partners - Analyst*

Moving to the service -- on the services side. Will that put you into competition with any of your service provider customers?

Dan Ryan - *Secure Computing Corporation - CEO*

Not that we're aware of. We have some MSP partners that provide services. In fact, we would see an opportunity to actually license our services through other partners that could actually sell those services. We have no issue private labeling some of these hosted security services, if that makes sense.

Josh Jabs - ***Roth Capital Partners - Analyst***

And then specifically on the OEM side with some of your services. I know you've expanded that quite a bit here this spring, but can you just give us some color on how that's going?

Dan Ryan - ***Secure Computing Corporation - CEO***

Could you repeat that?

Josh Jabs - ***Roth Capital Partners - Analyst***

The OEM with the partnerships specifically for TrustedSource?

Dan Ryan - ***Secure Computing Corporation - CEO***

We continue to go down that path. I think we have several partnerships. I would say our most active partnerships are less around TrustedSource and more around virtualization and also working with Riverbed in some joint solutions. I think that the TrustedSource alliance we have had out there -- we continue to market that and to sell that and we're active there. I don't think that's a big revenue opportunity for us in the near term.

Josh Jabs - ***Roth Capital Partners - Analyst***

Okay.

Tim Steinkopf - ***Secure Computing Corporation - SVP of Operations & CFO***

I think in a broad sense, we believe that -- and I think that quite a bit of the market or IT pundits would agree that eventually reputation-based technology is going to be a clear driver or gating factor for activity on the web, and TrustedSource is a leader there. It's best for us to continue the broad capture of data such that we can maintain TrustedSource as the true leader in that reputation based arena.

Dan Ryan - ***Secure Computing Corporation - CEO***

That's another good point where we see synergy and consolidation between web and mail. We have TrustedSource reputation information now includes web reputation, malware, again mail reputation as we always have. And as we get into the cloud and all of a sudden have thousands more points of reference and data collection, because of our customers are going through the service. We just get that much more visibility on the data that's out there that we can correlate.

Josh Jabs - ***Roth Capital Partners - Analyst***

Last question. A little bit of the shift in focus here, and the cost reductions cause a change in the comp structure that you recently introduced for your sales team?

Dan Ryan - ***Secure Computing Corporation - CEO***

No, it will not. The comp structure with the emphasis on new business development and cross selling remains intact.

Josh Jabs - *Roth Capital Partners - Analyst*

Okay. Great, thanks.

Dan Ryan - *Secure Computing Corporation - CEO*

It's definitely having an impact.

Operator

Sarah Friar with Goldman Sachs, your line is open.

Fred Green - *Goldman Sachs - Analyst*

Hey, this is Fred [Green] for Sarah. You're taking a pause in paying down your debt right now. How long do you expect before you resume paying it down and is there a certain amount of cash you're looking to keep on your books going forward?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Yes, we have taken a pause, Fred, and the big reason we took a pause is because of the macroeconomic environment. And again, we just saw this macro environment and said maybe it would be better to put that cash on the balance sheet. I think -- although we have not determined an exact level of what we want on a balance sheet before we start paying again, I think somewhere between $25 million and $50 million. And that will be a discussion we have with the board on an ongoing basis. And then I think once we build it up to a certain level, we'll consider paying down more or maybe we'll build it up to a certain point where we can pay down some big chunks at certain time levels. For the near future, we're going to be putting the money on the balance sheet for now.

Fred Green - *Goldman Sachs - Analyst*

Okay. Great, and do you have an update on sort of how long you think it will be until you have a workaround for the Finjan patents?

Dan Ryan - *Secure Computing Corporation - CEO*

I don't know that -- I'm not going to talk about a workaround. We have the ability immediately to ship a product without the piece of the product that is alleged to infringe. We don't agree it infringes, but if we were caused to, we could ship a product without that. It's one type of detection mechanism among many on the product, and we can ship without that.

Fred Green - *Goldman Sachs - Analyst*

Thanks a lot.

Operator

Joe Maxa with Dougherty and Company, your line is open.

Joe Maxa - *Dougherty & Company - Analyst*

Regarding your SafeWord and your narrowing your focus to the remote access solutions, does this mean you're effectively taking yourselves out of the larger consumer authentication opportunities?

Dan Ryan - *Secure Computing Corporation - CEO*

I think when we say focused, we have some of the largest deployments in the world too. So it's a little bit of a dichotomy. But with SafeWord 2008 and really the successful no touch channel we've built around SafeWord and Microsoft deployments, we're going to continue to put a lot of the focus there. That's what is growing well for us. That's what has the best channel progress right now and that's the one that we think we have some uniqueness. Our product rolls out in that environment very easily, much more readily than most products, and this is where the marketing focus would be, I'd say. I guess we'll still continue to sell into accounts we're in. This is where we see a nice, steady predictable growth through a relatively low-touch channel.

Joe Maxa - *Dougherty & Company - Analyst*

Are you see any changes in the market that will keep you from more aggressively going after the hardware token side?

Dan Ryan - *Secure Computing Corporation - CEO*

We do the mobile [pass-type] electronic token which of course everybody's anticipated would be replacing tokens and that has not come to fruition. We still have a vast majority of the business goes with physical tokens, and we haven't seen a substantial change in our business, at least right now. We keep anticipating we'll move to other forums. We're very aware of that, but it hasn't happened yet.

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

What Dan just said is may be the key item to both questions you asked, Joe, and as much as we continue to look for consumer opportunities, or et cetera, the token market is not evolving that quickly. It seems like remote access tokens is still the leading solution and the market has not really embraced the next step or the next direction. So, what we want to do currently is try and capitalize on that and make the most of that. In the meantime, we will certainly be paying attention to where does that next path really show up. So that we can then jump into that. At present, tokens, remote access, business enterprise, is still the leading drivers in that part of the market.

Joe Maxa - *Dougherty & Company - Analyst*

Great, thanks a lot, guys.

Operator

Katherine Egbert with Jefferies, your line is open.

Katherine Egbert - *Jefferies & Company - Analyst*

Hi, I think before you answered the question about what positions you cut and you said it was mainly services. What planned positions did you eliminate?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

I'm sorry, Katherine, you must be on a mobile. You're cracking up. We did eliminate services and you said what?

Katherine Egbert - *Jefferies & Company - Analyst*

What planned positions?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Oh, planned positions. Planned positions was a little bit more across the board. We're not seeing quite the level of growth that we have been planning on, and the plan, of course, had been kind of not -- it's not a perfect peanut butter spread across the whole organization, but it was spread across the whole organization. So the planned position was a little bit more evenly spread across the board.

Katherine Egbert - *Jefferies & Company - Analyst*

Thanks.

Operator

Eric Suppiger with Signal Hill, your line is open.

Eric Suppiger - *Signal Hill Group LLC - Analyst*

Good afternoon.

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Hey, Eric.

Eric Suppiger - *Signal Hill Group LLC - Analyst*

Did you give the headcount earlier?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

No, but I think post the actions we've took this week, we should be right around 900.

Eric Suppiger - *Signal Hill Group LLC - Analyst*

And I presume at the end of the quarter it was 975? So all of the cuts have been done at this point?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Yes, substantially, yes.

Eric Suppiger - *Signal Hill Group LLC - Analyst*

Okay, can you give us a little feel -- I guess I'm trying to understand what parts of the firewall market you're going to be redirecting your focus away from?

Dan Ryan - *Secure Computing Corporation - CEO*

Well, I think I would say we don't feel that we are probably a strong competitor in the general network firewall space horizontally, right. That's not our strength. We are much more specialized in high-value data, high-value applications. And in many cases our firewalls are used behind other perimeter firewalls. So I think what we're saying is that our development effort is going to be to double down where we win today. And we do a fantastic job in federal government, in financial services, and utilities in other areas where we're protecting high value applications and data, and I think it's easy for us to find ourselves competing with network firewalls. It's easy to get drawn into those fights against the big firewall players.

And I think we want to pick the fights where we can win and really go aggressively after those instead. We don't want to find ourselves in every network deal. We want to be in the deals where they're high value and high margin and we have a layer 7 orientation, an application layer orientation where we have a 3 out of 4 chance of winning, not a 3 out of 4 chance of losing.

Tim Steinkopf *- Secure Computing Corporation - SVP of Operations & CFO*

To add on briefly, we're going to compete with the same people, if it's a layer 3 or 4 deal. If it's a perimeter network deal, as we compete with when it's a layer 7 deal. When it's in front of an Oracle server or application et cetera. We're certainly going to compete. But we have a much better chance to win when it's a layer 7 oriented-type of project and that's where we really want to make sure. You get into those high assurance networks. That's where we're going to get a higher win ratio. So we're going to make sure we're really focusing in and competing in as many of those as possible.

Dan Ryan *- Secure Computing Corporation - CEO*

The other thing we mentioned briefly that we're just embarking on, we announced this week some activities we're doing in virtualization. Our product is a software product, effectively running on a hardened black box, but this is very easily virtualized. We don't have a lot of semiconductor dependencies. So we have some unique capability where people need virtual firewall capabilities that many of the other competitors do not have, and depend on silicon and proprietary platforms.

Eric Suppiger *- Signal Hill Group LLC - Analyst*

Okay, and then can you help us a little bit in terms of measuring how your stronger-performing products are performing? Specifically, I'm talking about the web gateway and the mail security products. You're not breaking them out, so can you give us some way of gauging how your success in those areas is performing since that's arguably where the greatest investor interest would lie?

Dan Ryan *- Secure Computing Corporation - CEO*

We're not breaking them out now. We may chose to do that, however, in the future so there would be more clarity on that. I would just say what I did mention, is that Gardner has said the market rate is growing for web -- is the least penetrated at 15% with growth rates depending on whether it's appliance or wholesale somewhere between 20 and 36%. And I think that our recent history for Webwasher has been in excess of those growth rates. I would say mail is almost inextricably -- it can't be removed from web. I think it's becoming part of web, particularly related to the web 2.O protection opportunity with our SWAT program. Mail and web are a hybrid solution now, and we're seeing those will emerging more and more together in our eyes with our solutions. We'll probably talk about these together. We probably won't even separate. If we do more segmentation, it probably won't be to separate web from mail. It might be to separate web and mail from network and access.

Eric Suppiger *- Signal Hill Group LLC - Analyst*

As a sales strategy, are you moving away from bundling the firewall with either the web or the mail and just selling them on a bundled basis more often?

Dan Ryan *- Secure Computing Corporation - CEO*

We still sell the firewall as the right solution to put in front of our other gateways. Obviously, we try and put as many of our products in as possible, but I think that -- that's a different procurement in many cases. So there's just more synergy with web and mail and I think from a cloud perspective, having a hosted offering, having the flexibility of having remote offices or home or internet cafe users going through the cloud and people at corporate going through the appliance. We see a more natural synergy between mail and web services.

Eric Suppiger *- Signal Hill Group LLC - Analyst*

Last one, is there much cost associated with the infrastructure for the hosted service?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Yes, there's cost, of course, in rolling it out. And hopefully there's going to be a lot of costs because it will be so successful that we'll need a lot of capital and pipes going in. But we do have, I believe seven data centers around the world today that support our TrustedSource environment, so we're quite familiar with this. It's not like we're a startup diving into this for the first time. So it really is layering on hardware and software infrastructure in those data centers and in some cases increasing the pipestone.

Dan Ryan - *Secure Computing Corporation - CEO*

We have that in our plan. That's in the budget that we described to you.

Eric Suppiger - *Signal Hill Group LLC - Analyst*

Very good. Thank you.

Operator

Thank you, our last question comes from Todd Raker with Deutsche Bank. Your line is open.

Todd Raker - *Deutsche Bank - Analyst*

Hey, guys, two questions for you, can you hear me?

Dan Ryan - *Secure Computing Corporation - CEO*

Yes.

Todd Raker - *Deutsche Bank - Analyst*

First, just looking at the balance sheet, it look like long-term deferred revenue kind of came down as a percentage here. Are you seeing shorter duration bookings and if so what's driving it, the economy?

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Actually yes to both. Yes, we did see a reduction in the longer term, and yes, when it was specifically cited as to why that would happen, the economy, budget dollars, cash flow was the most often-cited reason.

Todd Raker - *Deutsche Bank - Analyst*

And if I step back, you guys are clearly cautious with the outlook given the experience you had, but if I look more generally across the security space, the results by and large have been relatively robust. And it doesn't look like some of the larger companies in this space are seeing the same type of macro headwinds that you guys are.

Tim Steinkopf - *Secure Computing Corporation - SVP of Operations & CFO*

Well, what I would say is that there are certainly a few companies that have had some troubles, along with us. I would agree with you that there's been some that have not. The interesting thing for us is that if our government business had not run into troubles via the budgeting, et cetera, we would have hit our numbers. And therefore, we would have put up potentially exceeds numbers, maybe a little short on billings, but the rest of the numbers, revenue and earnings, et cetera, cash flow, would have all been at the high end, if not maybe even exceeded guidance. And it's interesting, in analyzing that situation, there's some people -- I'm not saying we're predicting this, but in analyzing the situation looking forward, there's at least some level of concern that the Q2 will be when the commercial markets really come home to roost. And I think you've seen that in the more conservative guidance headed into Q2. So some companies have made their Q1 numbers. They've got it conservatively for Q2. We would have been in that same boat if we hadn't had the double whammy of government as well. I think for us we're very much -- we are somewhat concentrating on government. We will also have that concentration in finance and banking, which of course they're suffering from macro factors as well. That would be our view of it.

Todd Raker - *Deutsche Bank - Analyst*

All right, thanks, guys, appreciate it.

Operator

I'll turn the call back over to Dan Ryan.

Dan Ryan - *Secure Computing Corporation - CEO*

Well, thank you for joining us and thanks for taking the time to ask the questions. Hopefully we answered them and look forward to updating you on our progress in three months. We remain optimistic on our business and hopefully we'll have something good to report in three months.

Operator

Thank you. This does conclude today's conference call. You may disconnect at this time.

Exhibit 6

Finjan's Corrected Explanation of IDC Report Calculations

in $M	2004	2006
IDC Estimated Finjan Revenue	12.9[a]	19.7[b]
Finjan Financial Statement Revenue	7.1[c]	8.4[d]
Difference[1]	5.8	11.3
Unadjusted Total Market Revenue	4,479.4[a]	13,237.1[b]
Adjusted Total Market Revenue[2]	4,473.6	13,225.8
Adjusted Finjan Market Share[3]	0.159%	0.064%
Total Finjan Lost Market Share 2004 to 2006[4]		0.095%
Percent of 2004 Finjan Market Share Lost by 2006[5]		60.0%

Explanation of Calculations

1 = (IDC Estimated Finjan Revenue - Finjan Financial Statement Revenue)

2 = (Unadjusted Total Market Revenue - Difference)

3 = (Finjan Financial Statement Revenue / Adjusted Total Market Revenue)

4 = (Adjusted Finjan Market Share 2006 - Adjusted Finjan Market Share 2004)

5 = (Total Finjan Lost Market Share 2004 to 2006 / Adjusted Finjan Market Share 2004)

Source Documents

a - Kobialka Decl. at Ex. 24 (PTX-25) at SC076372-74.

b - Kobialka Decl. at Ex. 27 at 5-8.

c - Answering Brief Ex. 15 at FIN009743.

d - Answering Brief Ex. 16 at FIN009700.

Exhibit 7

Home | Contact us | RSS | Search

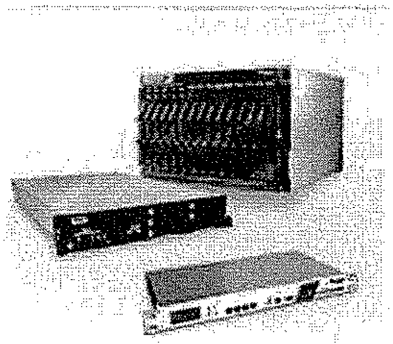
Quick Access

Products Solutions Security Center Partners Support Company News and Events

Home > Support > Technical Support Offerings

Support

- Overview
- Case Report Form
- Finjan Vital Knowledge
- Technical Support Offerings
- Professional Services
- Downloads
- Training Programs
- Support Notifications
- WEEE RoHS Policy



TECHNICAL SUPPORT OFFERINGS

The Finjan Commitment to Support

Finjan offers **secure web gateway products** for the enterprise market. Utilizing patented active real-time content inspection technology, Finjan's award-winning appliances prevent Crimeware and other malicious web content from infiltrating corporate networks and stealing business data. This technology allows Finjan to provide its customers with active real-time protection against zero-day and targeted web attacks (Crimeware, Web 2.0 attacks, spyware, phishing, Trojans, obfuscated malicious code, etc.), as well as other types of malware.

We at Finjan realize that efficient and responsive support for our security systems is critical to our customers' ongoing business operations. Our support commitment is based on sharing information, responding quickly to changing needs and working through problems and solutions together with our customers. Finjan's comprehensive support programs are aimed at preventing problems from occurring, and solving them swiftly if they do arise.

Your Choice of Technical Support Plans

Whether your company requires around-the-clock coverage or basic support, Finjan can deliver the level and types of support you need. Our tiered technical support plans offer flexibility and convenience to match your particular business needs.

Silver Support (Basic Plan)

Silver Support provides basic support coverage at no extra cost for the duration of your subscription. Silver Support offers timely and cost-effective response to your support needs, including the following:

- Guaranteed availability of Finjan technical support resources during local business hours
- 24/7/365 availability of online and email case reporting tools
- Access to Finjan Vital Knowledge™ - a centralized one-stop knowledge portal of technical support solutions
- Product upgrades, security updates and maintenance releases during the subscription period via auto-update feature

Gold Support (Enhanced Plan)

Finjan Gold Support is our enhanced support package, including unlimited 24/7/365 access to Finjan support specialists, available for additional fees during your subscription. Gold Support features the following services:

- Guaranteed availability of Finjan technical support resources and case reporting tools on a 24/7/365 basis
- Unlimited 24/7/365 telephone support
- Product upgrades, security updates and maintenance releases during the subscription period via auto-update feature
- Access to Finjan Vital Knowledge™ - a centralized one-stop knowledge portal of technical support solutions

Advanced Replacement Service (ARS) Option*

Finjan offers ARS as an additional fee-based service, including replacement of faulty hardware with a new or refurbished unit, shipped next business day following RMA approval.

NG-1000/5000 Appliance Series Return Material Authorization (RMA)

The problem reporting and support procedures for the NG-1000/5000 Appliance Series can be found under this link

NG-6000/8000 Appliance Series Advanced Replacement Service (ARS)

The problem reporting and support procedures for the NG-8000 Appliance Series can be found under this link

Technical Support Offerings - Feature Matrix

Service	*Silver Support*	*Gold Support*
Technical Support availability	Business hours as defined locally	24/7/365
Online and Email case reporting	24/7/365	24/7/365
Unlimited telephone support	Business hours as defined locally	24/7/365
Automatic download of product upgrades and fixes	✓	✓
Ongoing automatic security updates from Finjan Malicious Code Research Center (MCRC)	✓	✓
Immediate notification of case closure	✓	✓
On-site support available (optional)	✓	✓
Access to Finjan's online technical resources	✓	✓
Escalation path available	✓	✓
Standard hardware warranty	1 year	1 year
Advanced Replacement Service (ARS)* option including extended warranty	✓	✓

* Series NG-8000 and NG-6000 hardware support supplied by IBM (coordinated thru Finjan).

Privacy Policy

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on May 16, 2008, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

BY HAND DELIVERY AND E-MAIL

Frederick L. Cottrell, III, Esq.
Kelly E. Farnan, Esq.
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
cottrell@rlf.com; farnan@rlf.com

I hereby certify that on May 16, 2008 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.
Christopher A. Seidl, Esq.
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
jmholdreith@rkmc.com ; caseidl@rkmc.com

/s/ Philip A. Rovner
Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P.O. Box 951
Wilmington, Delaware 19899
(302) 984-6000
E-mail: provner@potteranderson.com